保安資訊
SAVETIME
INFORMATION SECURITY

Symantec Endpoint Detection and Response
迅速的威脅搜尋及矯正方式

保安資訊：賽門鐵克解決方案專家

地址：台中市南屯區三和街150號
電話：0800-381500・04-23815000
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

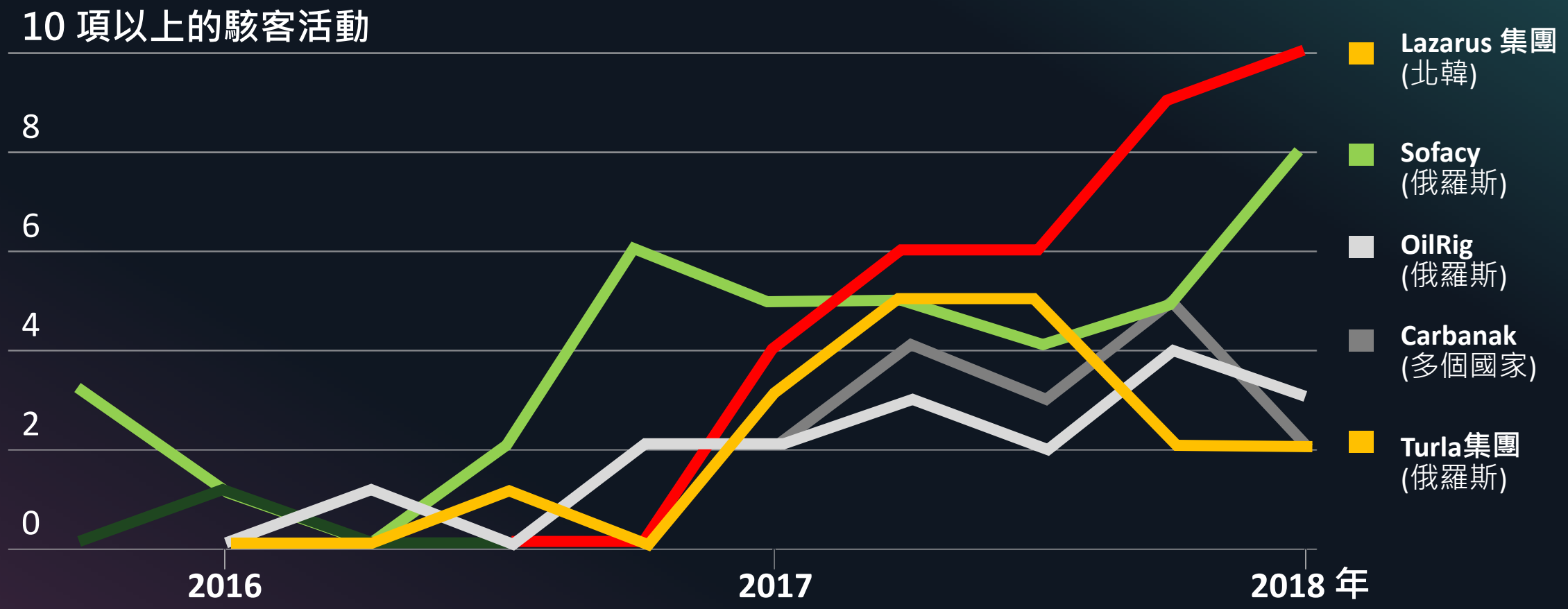
保安資訊

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的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到可用的資源。

BROADCOM SOFTWARE

駭客團體攻擊增加



附註：駭客團體的國家關聯性，是以網路安全公司假設的關係或地點為依據。
資料來源：AlienVault

華爾街日報 (THE WALL STREET JOURNAL)

保安資訊 SAVETIME INFORMATION SECURITY

彙整資安事端回應趨勢

191

攻擊者停留在客戶環境
的平均天數

53%

企業表示網路安全
技術短缺

38%

時間由 SOC 團隊
用於對抗警示

27%

機率入侵
會在兩年期間再次發生

越來越多攻擊者利用合法工具「就地取材」，感染過程近乎無症狀

保安資訊 SAVETIME INFORMATION SECURITY

雲端世代最佳端點安全產品組合

保護新興威脅

- 進階機器學習
- 為分析
- 降低記憶體攻擊風險
- 調適防護功能
- 模擬器
- SEP Cloud

偵測與回應

- 搜尋入侵指標 (IoC)並矯正
- 端點行為紀錄(錄影)
- 無檔案攻擊防護
- 沙箱
- 涵蓋端點、網路以及電郵的多面向威脅關聯性分析
- EDR Cloud

端點安全強化

- 應用程式攻擊面可視性
- 弱點評估與風險分類
- 隔離不受信任應用程式
- 應用程式防禦

主動式安全

- 部署欺敵工具 (即誘餌)
- 強化能見度揭露攻擊者及其意圖和戰術
- 高質感告警
- 全局式欺敵佈署

封鎖常見威脅

- 防毒引擎
- 檔案信譽
- 入侵預防
- 應用程式與裝置控管
- Power Eraser修復和矯正工具
- 開放 API

行動裝置端點安全

- 大規模的使用者社群威脅情報
- 行動惡意程式偵測
- 網路威脅保護
- 漏洞利用保護

保安資訊 SAVETIME INFORMATION SECURITY

SEP：業界最完整的端點保護

有效封鎖目標攻擊與零時差威脅的多層次防護技術

與時俱進，版次推升功能

獲得專利的即時雲端查詢功能  **用以掃描可疑檔案**

網路防火牆與入侵預防	應用程式與裝置控管	降低記憶體攻擊風險 (Enhanced)	信譽分析進 (Enhanced)	進階機器學習 (Enhanced)	模擬工具	行為監控 (Enhanced)	網路防火牆與入侵預防
在惡意軟體擴散到電腦並控制流量前，便加以攔截	控管檔案、系統登錄、裝置存取和行為，以及白名單與黑名單等等	攔截零時差攻擊，阻止其攻擊常用軟體的弱點	運用社群的智慧，判斷檔案和網站的安全性	針對新興和進化中的威脅進行執行前偵測	虛擬機器可使用自訂套件偵測隱藏的惡意軟體	監控並攔截出現可疑行為的檔案	在惡意軟體擴散到電腦並控制流量前，便加以攔截

入侵 → 感染 → 侵擾與洩漏

保安資訊 SAVETIME INFORMATION SECURITY

多層次的單一代理程式端點防護

Symantec Endpoint 產品組合提供最先進的技術

Symantec 單一代理程式

防惡意軟體	進階惡意軟體防護	欺敵技術	強化功能	EDR
• 使用全球最大規模的民間 GIN 封鎖常見威脅 • 封鎖橫向移動和指令及控制流量 • 裝置層級控制及鎖定 (USB、系統檔案) • 矯正惡意軟體感染	• 最有效的勒索軟體防護 • 防禦對抗無檔案威脅，包括對記憶體的刺探利用 • 針對關鍵漏洞進行虛擬修補 • 封鎖多形態的惡意軟體	• 識別身分隱藏攻擊者 • 暴露攻擊者意圖及戰術以強化安全態勢	• 自動評估應用程式風險 • 保護 IT 核准的應用程式，避免遭到刺探利用 • 隔離可疑應用程式，避免執行權限作業 • 在 Active Directory 停止持續威脅	• 偵測隱藏威脅 • 調查及搜尋 IoC • 快速修正端點 • 自動化 IR 任務

保安資訊
SAVETIME
INFORMATION SECURITY

賽門鐵克多層端點防禦對抗威脅

單一代理程式 | 整合式 | 單一代理程式

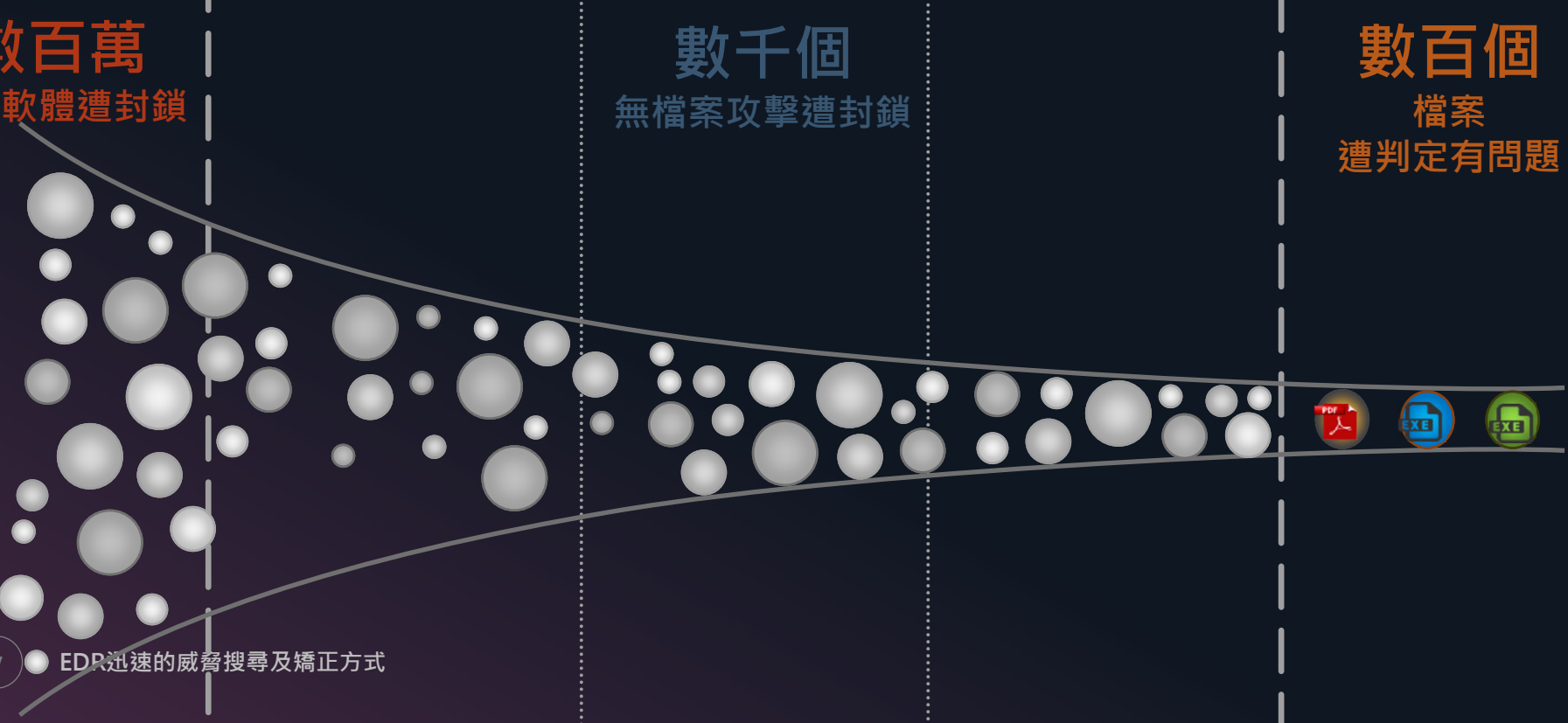
防惡意軟體 | 新興威脅防護 | 惡意軟體分析 | EDR

預防
已知威脅

進階防護及強化功能
- 應用程式控制
- Threat Defense for AD
- 欺敵技術
- 應用程式隔離
- Cloud Connect防禦

自動化
沙箱提交

資安事端
回應



保安資訊
SAVETIME
INFORMATION SECURITY

Symantec EDR 概述

偵測隱藏威脅

獲得警示掌握「隱匿行蹤」的威脅

搜尋及調查 IoC

尋找可疑物件、檢測、判定及遏止

快速修正端點

按一下即可矯正受影響端點

自動化及整合

提升各層級分析師的生產力

Symantec EDR 提供事件調查及回應功能，涵蓋 Windows、macOS 及 Linux。

保安資訊
SAVETIME
INFORMATION SECURITY

SOC/CIRT 團隊面對的關鍵問題

搜尋後威脅仍會持續存在

不連貫的遙測收集

- 需要手動相互關聯
- 情報摘要有限
- 誤報

目標式攻擊集團

- 攻擊者隱藏在正常活動中
- 難以識別 APT，需要少見的網路技術

有限端點能見度

- 調查人員缺乏詳細能見度
- 偵測進階攻擊方法的能力有限

不完整端點矯正方式

- 攻擊物件仍留在端點
- 攻擊在調查期間持續擴散

複雜的人工工作流程

- 複雜的人工調查流程
- 在控制及 SOC 整合方面缺乏協調

傳統危害偵測

偵測

不連貫的偵測與遙測收集，有限情報

單獨的掃描

端點　電子郵件　代理

沙箱　異常登入

缺乏全球情境

＋

手動相互關聯
及
有限情報

缺乏 AI 專業知識
和技術純熟的威脅研究人員

＝

- 能見度缺口
- 過多誤報
- 更長的威脅停留時間
- 非最佳偵測

保安資訊 SAVETIME INFORMATION SECURITY

EDR 及目標式攻擊分析

偵測

持續雲端串流分析，採用賽門鐵克 AI + 威脅研究技術

SEP
遙測

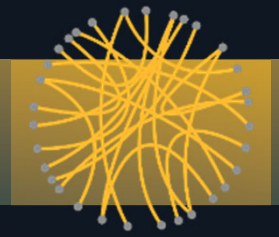
詳細收集

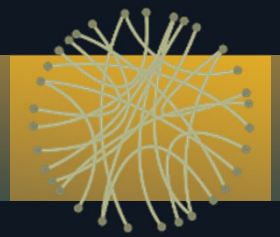
涵蓋整個企業

涵蓋所有企業

資料湖

全球遙測及
雲端型分析





1 研究人員遙測識別攻擊方法及物件

2 AI 導向分析依據研究人員資料集進行訓練

3 新攻擊是以建立新 AI 的方式找出 (訓練前使用)

4 分析師確認客戶環境遭到攻擊

5 資安事端傳送至 EDR 主控台
- 攻擊者詳細資料
- 受影響系統
- 引導回應

New and Unknown Threats

0
CYNIC DETECTIONS

0
INSIGHT DETECTIONS

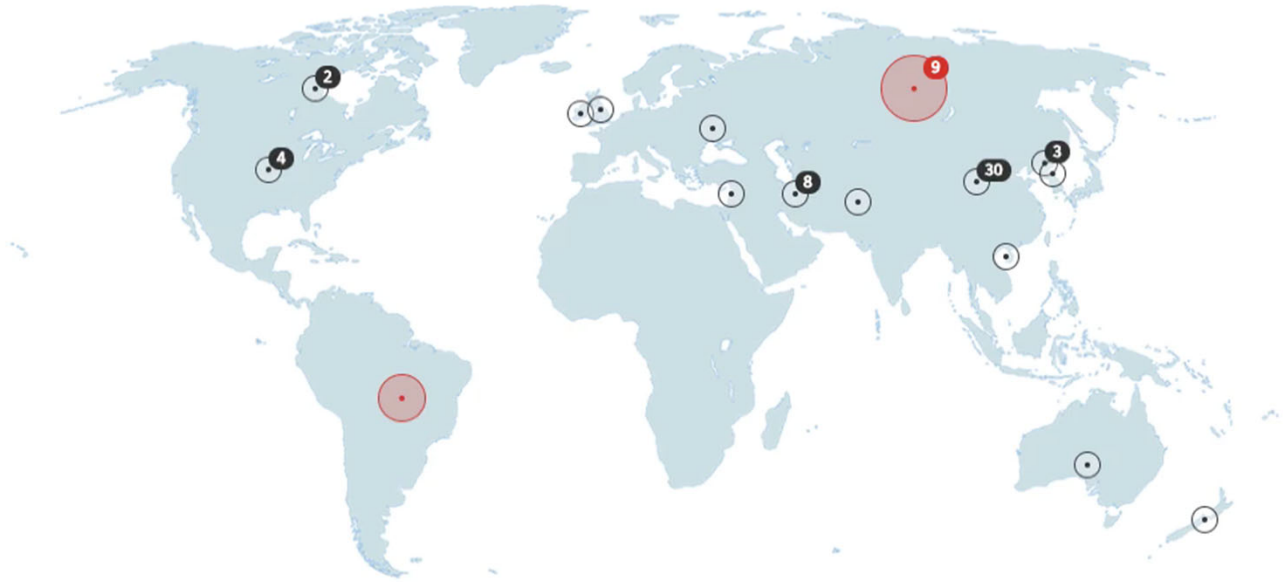
0
TOTAL DETECTIONS

No data available.

Endpoints

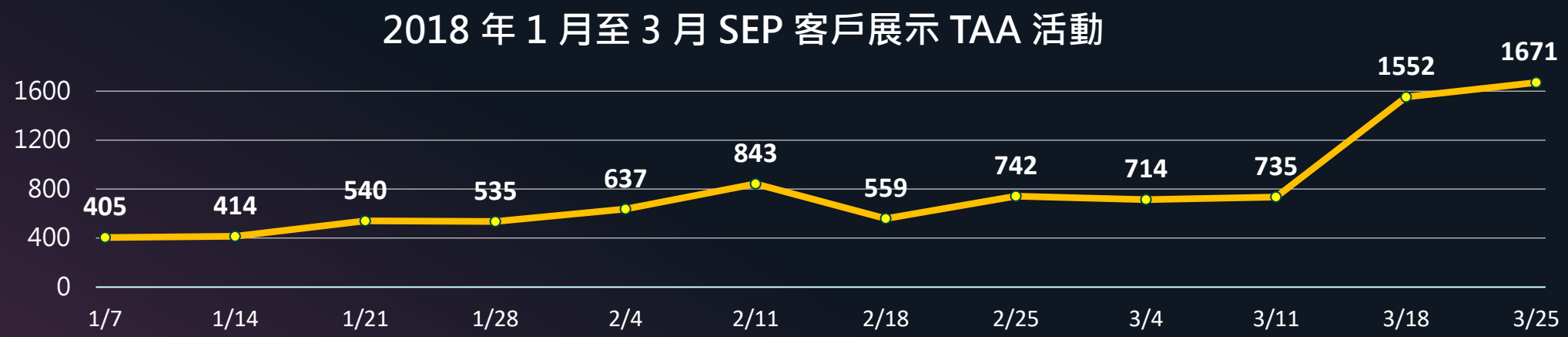
Active Endpoints at High Risk	Active Managed Endpoints
1	2

Global Adversaries by Location



目標式攻擊分析—證明價值

遭暴露的攻擊者團體					
					
Treehopper	Dragonfly	Shamoon	Thrip	Seedworm	Elfin
2017 年			2018 年		
3 月	5 月	12 月	1 月	年 2 月	年 3 月



異常偵測

偵測

以整體方式檢驗端點資產尋找異常狀況

概述

- 偵測有別於基準活動的異常情況
- 針對檔案、IP 及網域信譽套用多項情報摘要
- 時間表及路徑分析可偵測不規則的檔案安裝及程式執行地點
- 以數百萬個正常與惡意檔案為基礎的神經網路式機器學習

偵測軟體、記憶體、使用者及網路的異常情況

軟體 – 揭露安裝罕見軟體、搭載老舊或未修補作業系統版本的端點

記憶體 – 運用鑑識檢驗偵測記憶體內的不速之客

使用者 – 以行為分析偵測偽裝成合法使用者的攻擊者

網路 – 以統計分析識別異常 IP 位址

端點能見度有限

調查人員需要回應的重要問題

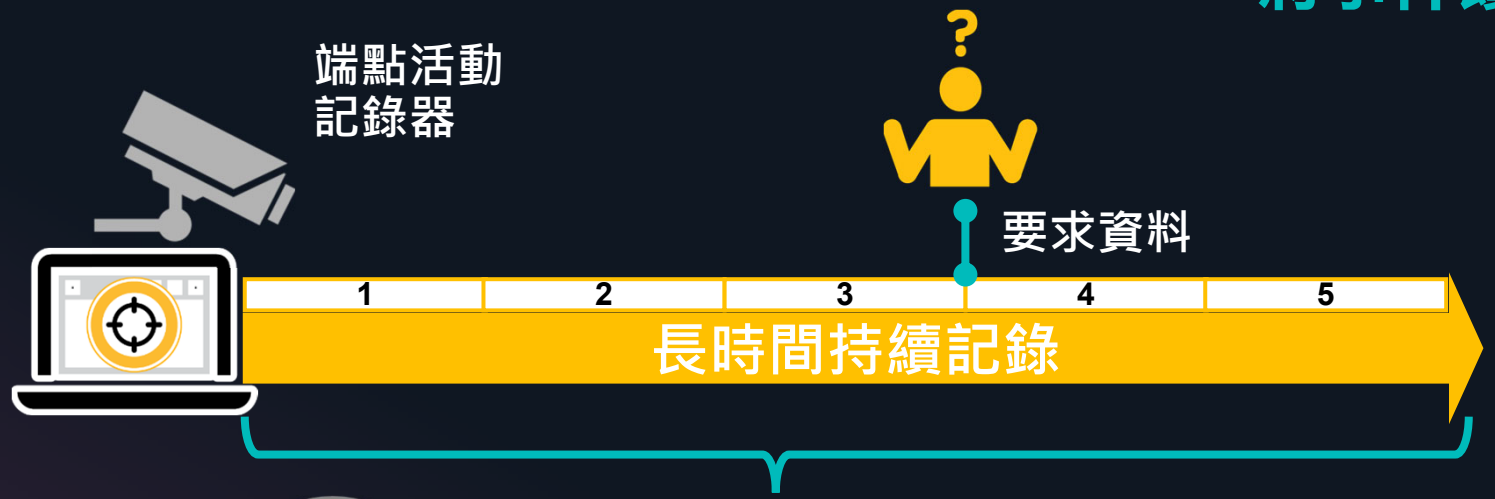
- 我的端點發生了什麼事情？
- 哪些檔案遭到使用，檔案來自何處？
- 惡意軟體是否擴散至其他端點？
- 我的端點有哪些程序遭到變更？
- 攻擊者是否在端點建立持續性攻擊？

保安資訊 SAVETIME INFORMATION SECURITY

端點記錄及播放

調查

掌握威脅對端點進行的系統及程序變更
將事件饋送至雲端型分析進行自訂偵測



擷取及播放本機佇列一切可用的項目

針對記錄事件執行自訂分析，
建立自訂偵測及警示

事件類型	事件描述
階段作業	使用者階段作業登入及登出
流程	啟動及終止
模組	載入及卸載
檔案	建立、讀取、刪除、重新命名
資料夾	資料夾作業
登錄碼	在登錄碼的作業
登錄值	在登錄值的作業
網路	行動者程序網路
已命名物件	已命名物件屬性

調查、搜尋及排定優先順序

尋找可疑物件及相關事件

端點 IoC 搜尋

- 在資料庫及端點即時搜尋 IoC
- 搜尋端點活動記錄器串流事件
- 利用快速過濾器
- 客戶延伸掃描區域 (例如 \Downloads、\Box)

鑑識收集

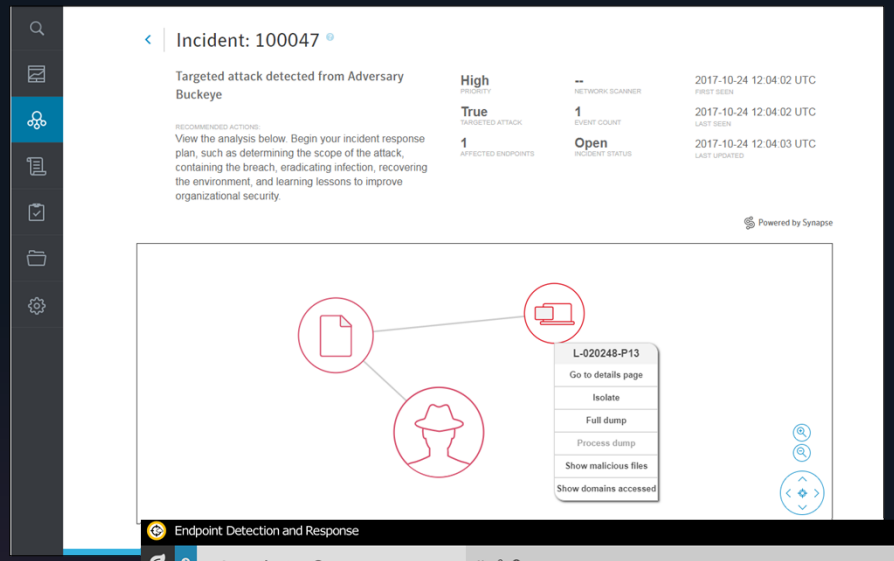
- 完整端點及檔案/程序傾印
- 取得程序記憶體
- 收集 PE 及非 PE 檔案
- 取得 OS 鑑識跡象 (例如預先擷取、MFT、Brower 歷史記錄)

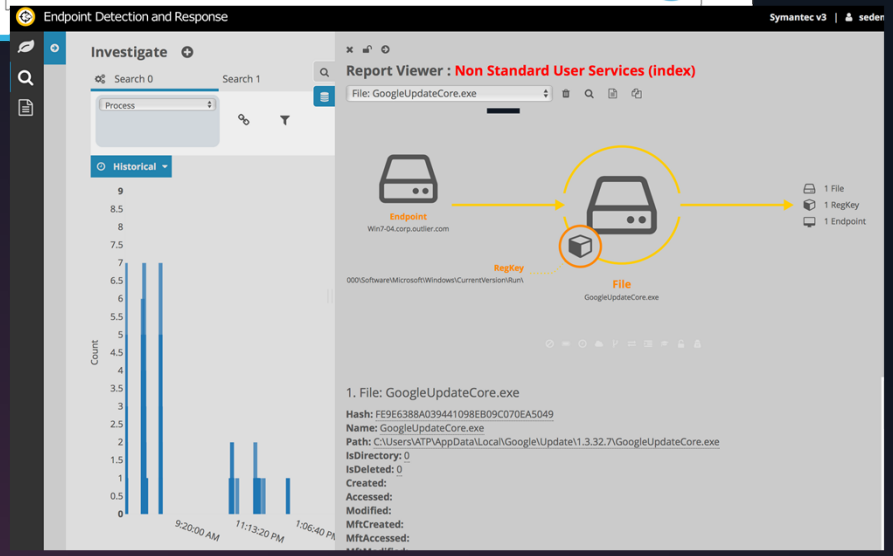
即時自動資安事端產生/沙箱

- 偵測記憶體刺探利用
- 可疑的 PowerShell
- 評定風險分數的記錄器事件
- 自動提交可疑檔案至沙箱 (內部部署或雲端)

視覺化 調查

互動式圖形可簡化複雜調查





- **視覺資安事端圖表及警示**
  - 將受影響端點與行動者及物件連結，作為中心探索更多詳細資料
  - 迅速得知資安事端的源頭、時間及影響
- **視覺連結分析**
  - 瞭解無關聯資料類型之間的情境關係
- **將大量資料轉換為互動式圖形及報告**
  - 以機器輔助分析聚焦於相關活動
  - 簡化報告

不完整的端點矯正方式

延遲訂定黑名單及遺漏攻擊物件，可能導致威脅重演

預防刺探利用擴散至其他端點：

- 調查期間無法隔離端點，造成攻擊擴散
- 延遲將檔案及網路位址加入黑名單，讓其他使用者處於風險之中

未修復的端點變更：

- 即使惡意檔案已遭刪除，載入點變更仍留存在端點
- 惡意程式碼注入登錄，再次造成記憶體攻擊

保安資訊 SAVETIME INFORMATION SECURITY

完整迅速的端點修復

回應

- 將檔案加入黑名單或許可名單
- 刪除檔案、倒轉載入點變更、讓端點回到感染前狀態
- 隔離受感染的端點
- 加強對抗未來感染

按一下就能從單一主控台完整矯正各端點。

保安資訊 SAVETIME INFORMATION SECURITY

複雜的手動工作流程

手動活動及程序妨礙 SOC 生產力

SOC管理員需要縮短解決問題的平均時間，並降低成本：

- 難以找到及留住技術純熟的分析師
- 必須加速分類並排定警示優先順序
- 需要擷取及重複使用技術純熟分析師的最佳實務準則，以強化資安事端回應及威脅搜尋

需要整合人員、程序及基礎架構以簡化作業：

- 簡化管理資料流程，並在各個控制點之間起始行動
- 需要讓現有的 SIEM 投資及問題單產品發揮更高效益

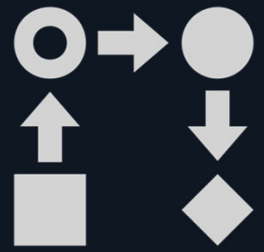
自動化調查及跡象收集

自動化

利用內建教戰守則，建立自訂工作流程

內建教戰守則

以內建教戰守則迅速發起網路安全功能，運用專業調查方法



自訂工作流程

將重複性的手動作業加以自動化，並建立自訂的調查流程。

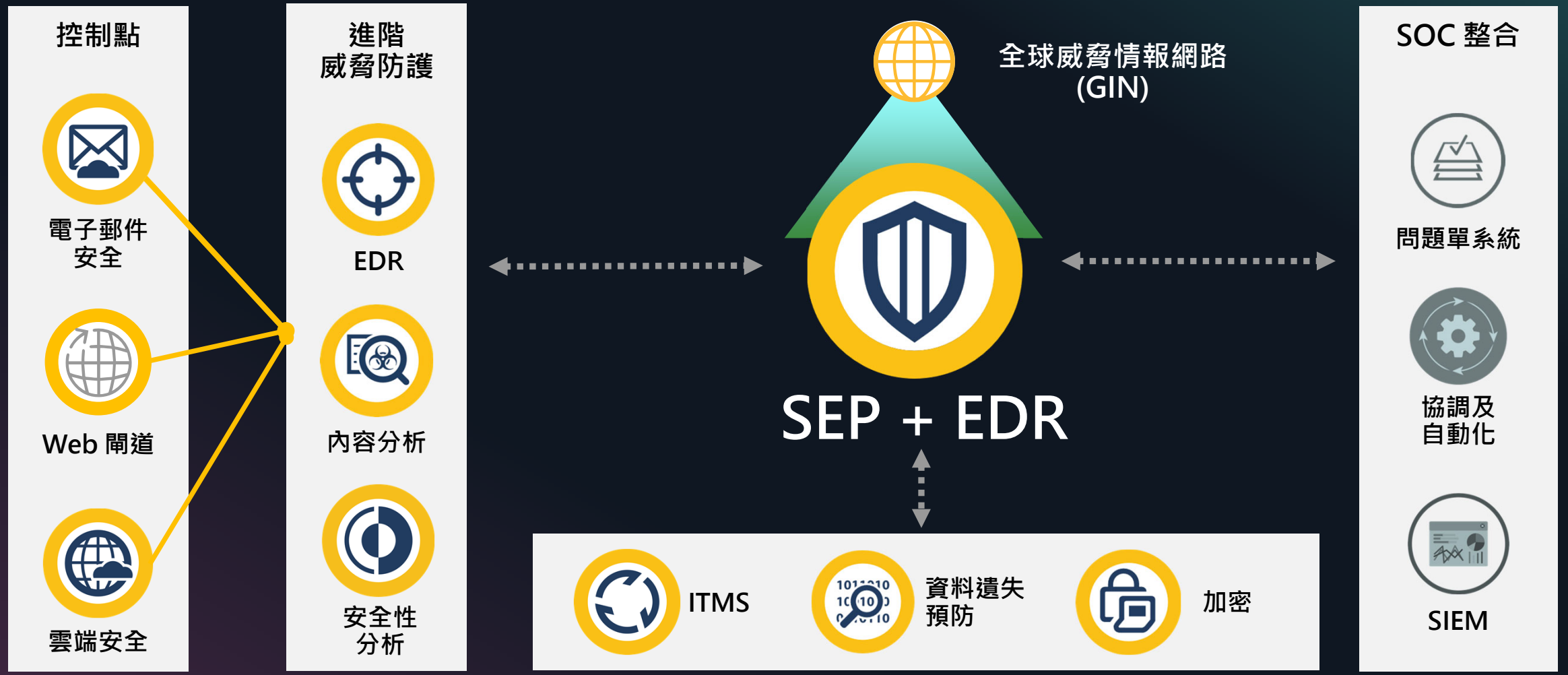
跡象收集

運用自動化跡象收集深入掌握端點活動。

與賽門鐵克及合作夥伴產品整合

整合

只有賽門鐵克提供整合式網路防禦



保安資訊
SAVETIME
INFORMATION SECURITY

摘要

賽門鐵克在 2018 年端點防護平台神奇象限領導者象限中獲得最具執行能力及最具前瞻性的願景完整度最高評價

圖 1 端點防護平台神奇象限 (Magic Quadrant)

資料來源：Gartner (2018 年 1 月)

Gartner

資料來源：Gartner, Inc.，端點防護平台神奇象限，Ian McShane、Avivah Litan、Eric Ouellet、Prateek Bhajanka，2018 年 1 月 24 日

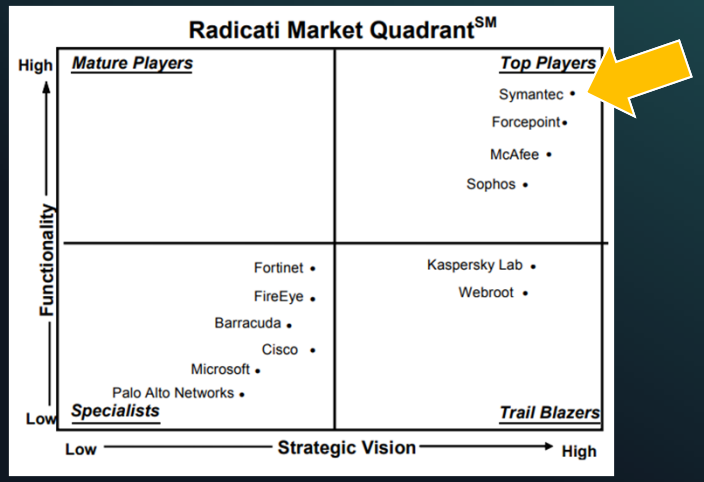
保安資訊 SAVETIME INFORMATION SECURITY

端點市場領導地位

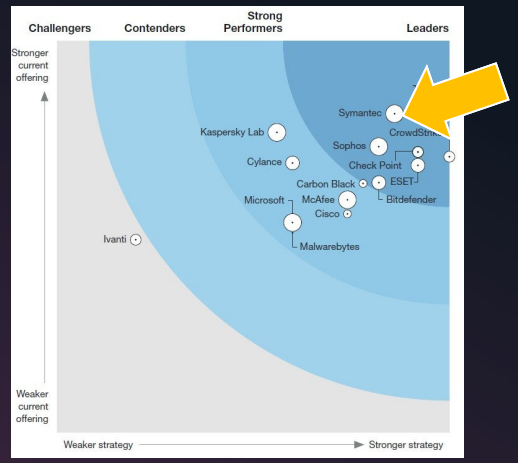
AV-Test 最佳防護獎得主
連續三屆

SE Labs

唯一連續 22 季榮獲
AAA 評等的廠商



2018年Radicati APT市場象限頂尖業者
(Market Quadrant Top Player)



Forrester Wave 2018年端點安全
套裝軟體評比領導者

SEP 14
SC MAGAZINE
推薦產品

SC 雜誌推薦
「我們喜愛這款產品。」

FROST & SULLIVAN

「賽門鐵克在 EPP 供應商之中的 EDR 市佔率居於領先地位。主宰端點市佔率」

全球端點安全市場2021 年預測

保安資訊 SAVETIME INFORMATION SECURITY

Symantec Endpoint Detection and Response

深獲肯定的客戶價值

1

單一代理程式攻擊

減少 IR 佇列及誤報

2

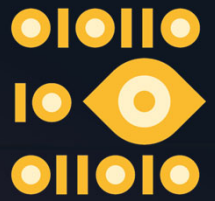
卓越的偵測分析

加速搜尋隱藏威脅

3

無可比擬的威脅情報

最大規模的民間情報網路



4

廣泛的 IR 自動化

迅速起始技術純熟分析師的實務作法

5

整合式網路防禦

在賽門鐵克及合作夥伴產品之間進行協調

保安資訊
SAVETIME
INFORMATION SECURITY

客戶使用案例

保安資訊
SAVETIME
INFORMATION SECURITY

大型付款處理商 – 整合代理程式

全球付款處理的領導廠商，支援數百萬家企業，每秒執行數千筆金融交易。

這家公司需要降低多個端點代理程式的成本及複雜度，並將端點防護擴展到數萬個端點，涵蓋 Windows、macOS 及 Linux。

需求

- 需要降低端點 8 個以上代理程式的複雜度
- 擴充支援數千個桌上型電腦、筆記型電腦及伺服器系統
- 運用包含 SIEM 在內的現有 SOC 基礎架構投資

解決方案

- 以單一代理程式因應防惡意軟體、新興威脅及 EDR
- 支援 EDR 功能，涵蓋 Windows、macOS 及 Linux
- 預建應用程式，適用於 Splunk 及 SOC 使用的其他現有工具

價值

- 簡化部署進階威脅及 EDR 功能
- 為 IT 營運及 SOC 團隊簡化廠商管理及支援
- 與其他已經使用的賽門鐵克解決方案協調，包括惡意軟體分析、網路鑑識及代理

保安資訊
SAVETIME
INFORMATION SECURITY

主要 NA 銀行 – 減少誤報

零售、企業及商業領域的領導銀行，擁有數百萬家客戶及上萬名員工。

這家銀行決定更換 EDR 產品，原因包括高誤報率，以及為了減少錯誤警報而建立的昂貴內部工具。

需求

- 因應現有 EDR 的中斷、效能及高誤報率等問題
- 降低內部工具的複雜度及營運成本
- 簡化各 Windows 版本的端點安全堆疊

解決方案

- 以單一代理程式提供保護及 EDR，並減少誤報
- 偵測無檔案攻擊和記憶體刺探利用，並記錄活動
- 廣泛支援 Windows 發行版，簡化堆疊

價值

- 減少管理多家廠商及自訂工具的營運成本
- 效力超越所有其他接受評估的廠商
- 利用預建應用程式，更容易與現有 SIEM 及問題單整合

大型付款處理商 – 整合代理程式

財星雜誌十大汽車製造商，是擁有 18 萬名員工的全球品牌。

SOC 團隊需要在攻擊入侵端點時採取立即行動，並需要將威脅可見度及回應行動整合至現有 SIEM。

需求

- 將重點放在鎖定高階主管及關鍵營運的進階威脅
- 將應變及矯正時間由數天縮短為數分鐘
- 利用現有 SIEM 部署投資

解決方案

- SEP 整合 EDR 降低誤報率，縮短應變時間
- 即時搜尋端點入侵指標，並記錄活動
- 與 SIEM 整合，提供單一主控台，因應能見度及回應需求

價值

- 整合廠商，降低成本及複雜度
- 以單一代理程式的多層防護提升成效
- 預建與 SIEM 及 Symantec Email Security 整合

感謝您！

保安資訊有限公司

資訊安全問題 解決專家

電話：

0800-381500・04-23815000

網站：

www.savetime.com.tw

保安資訊
SAVETIME
INFORMATION SECURITY

保安資訊
SAVETIME
INFORMATION SECURITY

背景

保安資訊
SAVETIME
INFORMATION SECURITY

新功能

新功能概述 – 融合 EDR

Symantec EDR 4.0

統合檢視資安事端

「我需要一個雲端型主控台，檢視 SEP 及非 SEP 端點的資安事端」

搜尋及矯正

「我需要由單一雲端型主控台針對端點進行搜尋及矯正」

統合調查教戰守則

「我希望自動化調查流程，涵蓋 EDR 之中的內部部署及雲端功能」

進階鑑識工具

「我需要進階工具搜尋注入、程序替換 (process hollowing) 及殼層程式碼」

Symantec EDR 提供資安事端調查及回應功能，適用於 SEP 及非 SEP 環境。

新功能概述(續)

專家引導

「我需要專家協助回應目標式攻擊資安事端」

進階攻擊偵測

「我需要揭露端點的進階攻擊技術」

MITRE ATT&CK 擴充

「我希望快速檢閱、比較及識別攻擊週期之中的缺口」

MITRE 網路分析

「我需要網路分析教戰守則，妥善偵測已知的攻擊者行為」

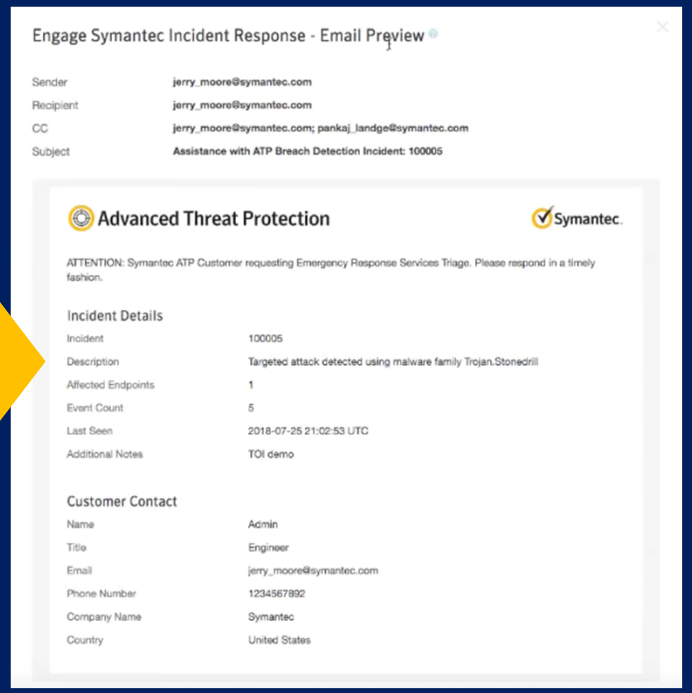
EDR 強化功能提供攻擊者分析、事件擴充、攻擊偵測及 IR 引導

要求專家協助

回應嚴重資安事端時因應專業缺口

利用新按鈕「參與賽門鐵克資安事端回應」

盡可能減少傳送給賽門鐵克的客戶及資安事端詳細資料



- 賽門鐵克 IR 人員分類資安事端
- 允許每項資安事端三封電子郵件
- 支援的資安事端 -
  - 目標式攻擊分析資安事端
  - 動態攻擊者情報 (Dynamic Adversary Intelligence) 服務資安事端
  - 利用沙箱判定檔案是否與已知目標式攻擊有關
  - 與已知目標式攻擊有關的電子郵件事件

行為攻擊偵測

運用 SEP 行為政策強制執行

- 由STAR團隊建立持續更新的行為模式
  - 詳述進行中的進階攻擊活動
  - 涵蓋相關行為，包括：
    - 檔案及登錄變更
    - 網路及程序活動
    - 使用特定 Windows API (例如建立執行緒)
- 針對需要進一步調查的技術提供安全分析師警告
  - 建立資安事端用於關鍵偵測
  - 已偵測 336 種新的進階攻擊技術

類　別	嘗試活動 - 範例
可疑程序	啟動、安裝、注入/替換、建立 exe、降低 sec. 警告、複製至資料夾/載入點、修改主機檔案
可疑的 PowerShell 或程序檔	網路存取、下載 exe、psexec 啟動
MS Office 可疑行動	啟動 bitsadmin、執行程序檔、執行排程作業、開啟 lsass、建立可執行檔或程序檔
可能的憑證竊取	存取 lsass 記憶體、不受信任的程序、加密 DLL 負載
已注入執行緒	網路通訊、啟動程序、建立自動執行項目、建立載入點

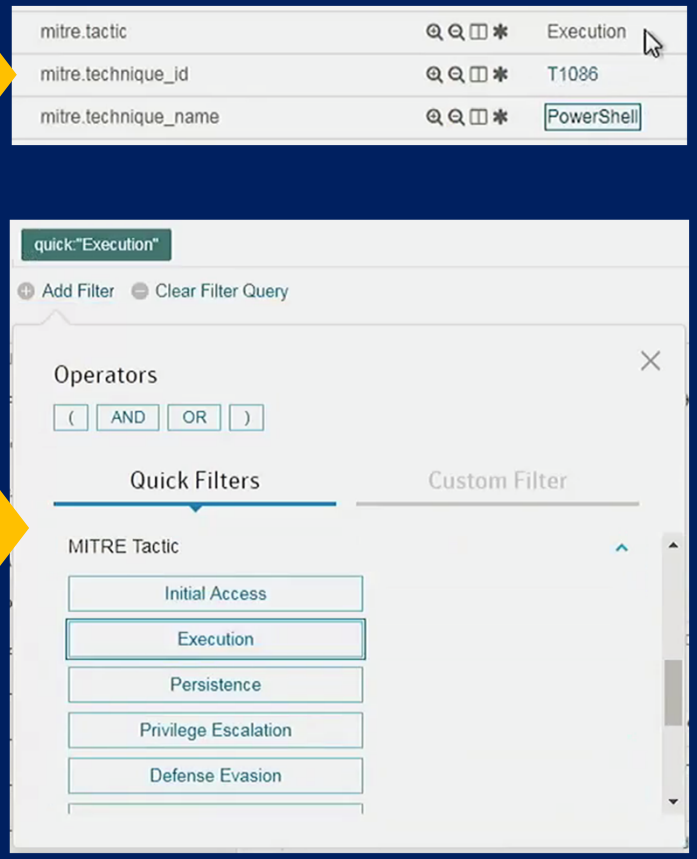
保安資訊 SAVETIME INFORMATION SECURITY

MITRE ATT&CK* 事件擴充

依據 MIRTE 戰術及技術名稱進行搜尋及篩選

擴充功能可詳述攻擊階段、技術 ID 及名稱

迅速以戰術、技術 ID 和名稱進行篩選



- 利用能見度掌握攻擊如何在端點進行
  - 檢視用於鎖定端點的戰術
  - 識別攻擊週期缺口
- 以 MITRE 屬性搜尋/篩選
  - 全新快速過濾器，適用於主控台事件及資安事端頁面
  - 連結至適當的 MITRE ATT&CK 頁面
  - 此版本支援 187 項 MITRE TTP 之中的 59 項

*攻擊者戰術、技巧及一般知識 (attack.mitre.org)

MITRE 網路分析

透過收集跡象的鑑識「事後」偵測實現零信任方法

MITRE CAR在雲端主控台實作
為調查教戰守則，產生資安事端

目前提供 ––

- 自動執行差異
- 可疑執行位置
- 可疑引數
- 透過載入程式庫進行 DLL 注入
- Powershell 執行
- 主機搜尋指令
- SMB 事件監控