everLEAP
金鐸科技股份有限公司

NTIMESEC

everLEAP
金鐸科技股份有限公司

關於ABouT US

- 擁有一群來自國內熟悉惡意程式分析、與駭客偵防技巧的專業人員
- 主要成員曾於政府與國軍資安主責單位，處理資安鑑識相關工作，組織型駭客行為與惡意程式分析上經驗豐富
- 技術團隊早於2014年便在臺灣設計、開發與提供MDR的服務模式為臺灣第一個提供Threat Hunting服務的國內MDR團隊

“即時反制所有威脅”

服務項目
SerVICeS

- 7x24 MDR服務 - ENDBLOCK
- 惡意程式偵測、處理及應變
- 網路威脅分析與獵捕服務
- 不限次數的資安事件處理與諮詢服務
- 資安事件鑑識與定期報告

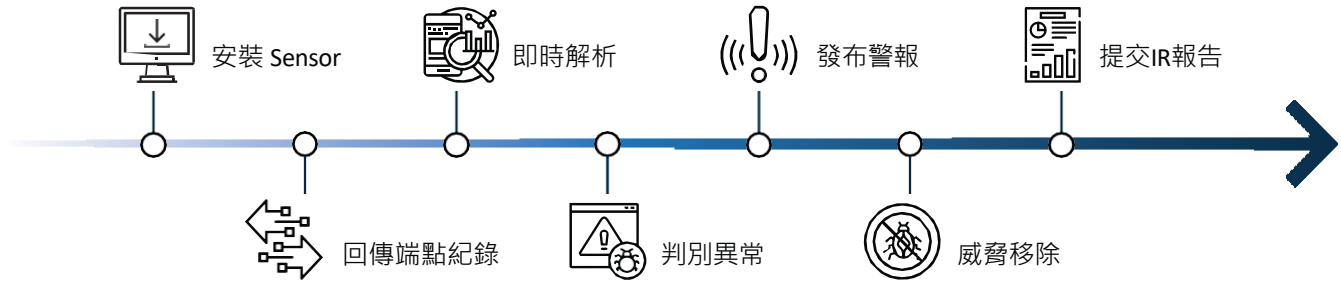
ENDBLOCK

最精準的主動式威脅獵捕服務
ProACTIVe THreAT HuNTING

隨著網路攻擊數量的高速成長，傳統的自動化反應機制，例如防毒軟體，已無法完全阻擋擁有專業技能的攻擊者。 必須透過專業的分析能力才能遏止網路犯罪的損失，已經是迫在眉睫的真實現況。 EndBlock擁有最完整的端點活動收集記錄，搭配自動而且高效的行為學習與分析系統，再加上擁有多年實戰經驗的資安事件處理與數位鑑識(DFIR)專家。 EndBlock已經成功在多次攻防之間，完美的擋下所有攻擊，從而與客戶建立良好的信譽。

EndBlock 服務流程

wORKFLOW



SOC v.s MDR優勢比較表

CoMPArISoN

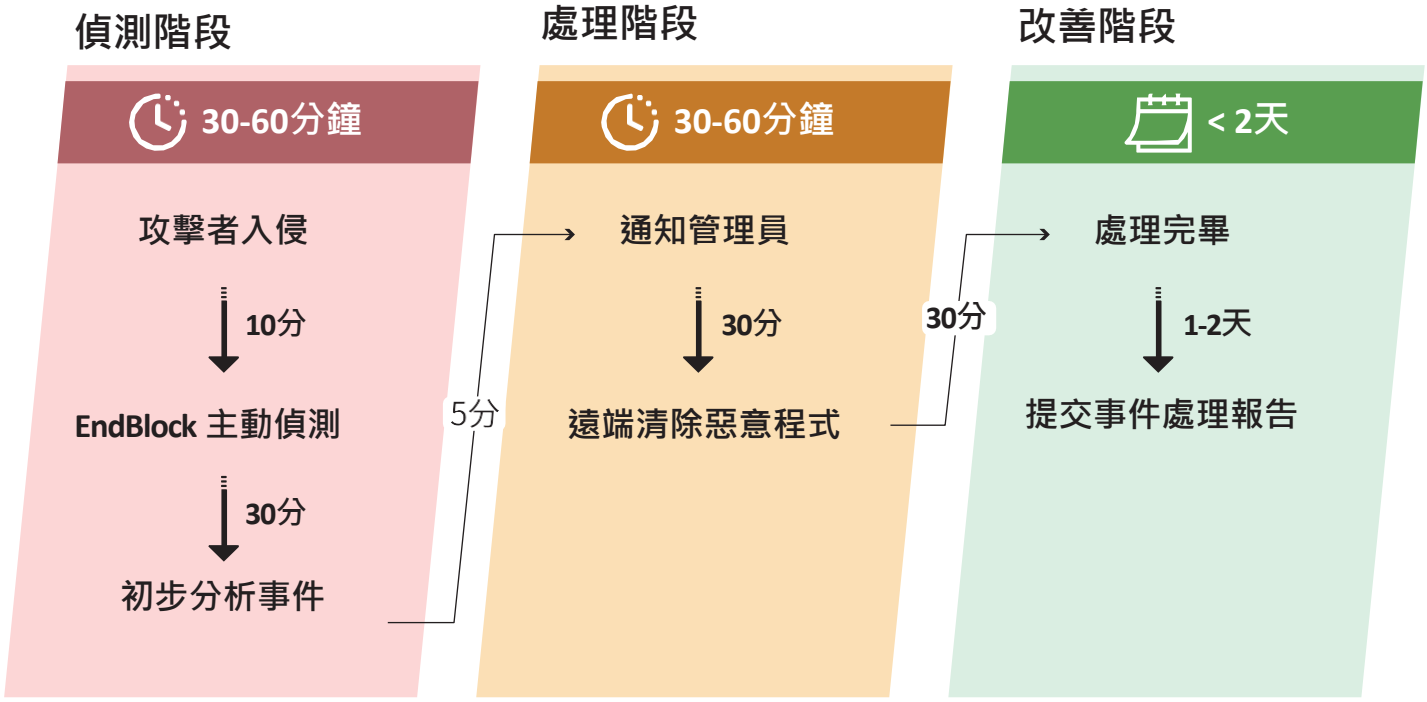
	MDR	傳統MSSPs
運作模式	威脅獵捕 (Threat Hunting)	資安監控 (Security Monitoring)
驅動模式	分析整體行為導向	警報分析導向
主要核心	Big Data + EDR	SIEM
處理目標	資安事件的回復與處理	偵測到的警報
處理方式	主動發現威脅	被動等待偵測
分析範圍	異常行為整體脈絡	警報本身
服務效益	徹底瞭解、回應及處理事件過程	判斷該警報是否要關閉或通報
評量準則	資料分析對於解決資安事件的幫助	警報的數量

“EndBlock 交付的是成效，不是大量警報”

EndBlock 提供全面性的偵測、分析、處理報告與改善方法
不僅僅是告知威脅，而是即時協助抵禦駭客攻擊，讓您沒有額外的調查負擔

EndBlock 處理流程-數量不受限

INCIDeNT reSPoNSe TIMeLINe



(數分鐘內即可開始主動獵捕並處理)

“及時偵測、即時防護”

端點搜集器基本需求

SYSTeM REQUIREMENTS

- 支援作業系統
  - * Windows 7 以上
  - * Windows Server 2008 R2 以上
  - * CentOS 7 以上
  - * Red Hat 7 以上
  - * Ubuntu 16.04 以上
  - * Debian 8 以上
  - * SUSE-SLES 12 SP3 以上
- CPU效能消耗 < 1%
- 網路平均每1000台頻寬消耗 1Mb/s
  *900台PC加上100台Server的平均值

金鐸科技股份有限公司
Everleap Technology INC.
TEL: 02-2249-0068
FAX: 02- 2247-6760
ADD: 新北市中和區中山路二段332巷17號13樓