www.intimesec.com

NTIMESEC

關於集時安全
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”

ITSEC MDR

有別於傳統分級式收費資安服務，ITSec MDR 為集時安全所推出的一站式解決方案，賦予企業端點設備全面性的保護，包括端點惡意行為分析、即時惡意行為通知與處理、事後報告與弱點修補建議，從根源阻斷威脅。

服務等級與項目
SERVICE LEVEL

對比看看您現有的資安廠商為您提供了什麼等級的服務呢？

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
分析	**通知**	**處理**	**報告**
7×24蒐集與分析端點行為提供即時威脅獵捕服務	判別惡意行為後立即通知客戶，提供即刻資訊、諮詢服務以應變攻擊	即時協助客戶應對攻擊，含刪除惡意程式、修改密碼、封鎖中繼站、攻擊來源等	提供根因分析報告，源頭追蹤、修補建議，確保未來不再發生

我們是全國唯一提供 7x24 等級 4、無限 IR 的 MDR 服務廠商

最精準的主動式威脅獵捕服務
PROACTIVE THREAT HUNTING

即時排除威脅

數位鑑識團隊 7x24 不間斷地即時監控、應變。隨時提供最專業的諮詢服務、最精準的警報

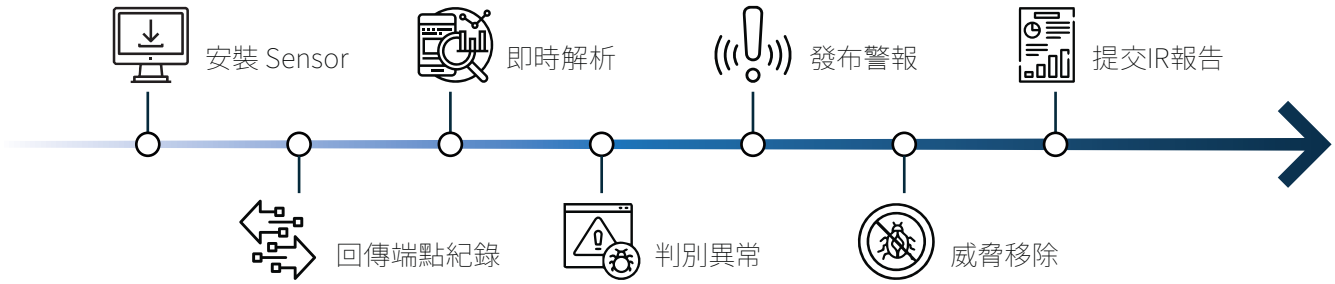
一站式服務

從偵測、分析、處理、溯源、鑑識報告到改善問題，ITSec MDR 一次性提供業界內最完整的服務範圍。客戶無須擔心後續的相關處理費用。

雲端原生

簡化部署投入的資源以降低營運成本，短短幾分鐘便可開始啟用保護

ITSec MDR 服務流程
WORKFLOW



SOC v.s MDR優勢比較表
COMPARISON

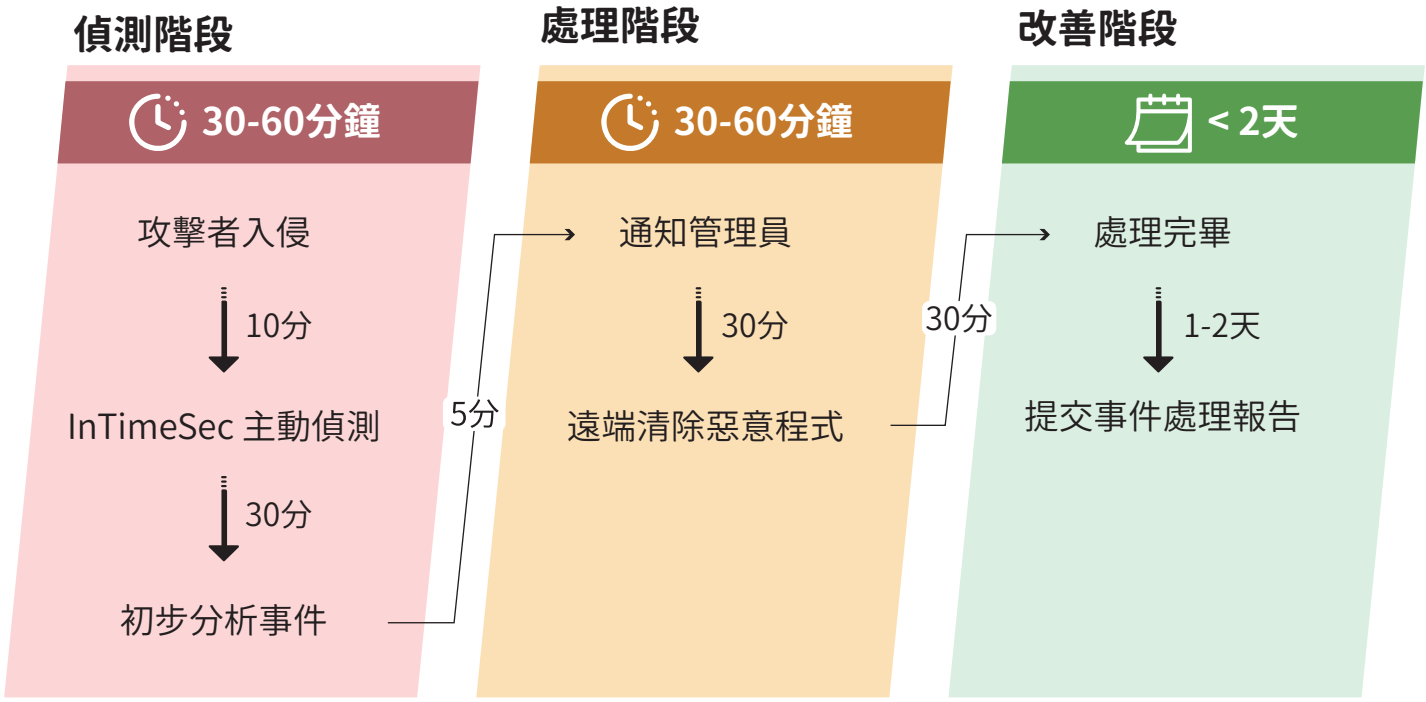
	MDR	傳統MSSPs
運作模式	威脅獵捕 (Threat Hunting)	資安監控 (Security Monitoring)
驅動模式	分析整體行為導向	警報分析導向
主要核心	Big Data + EDR	SIEM
處理目標	資安事件的回復與處理	偵測到的警報
處理方式	主動發現威脅	被動等待偵測
分析範圍	異常行為整體脈絡	警報本身
服務效益	徹底瞭解、回應及處理事件過程	判斷該警報是否要關閉或通報
評量準則	資料分析對於解決資安事件的幫助	警報的數量

“ITSec MDR 交付的是成效, 不是大量警報”

ITSec MDR 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

ITSec MDR 處理流程-次數不限

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

集時安全股份有限公司

INTIMESEC COMPANY LTD.

02-2712-0855
sales@intimesec.com
台北市信義區松山路130號7樓