

關於集時安全

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，在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 及 MDR 服務的國內團隊。

我們的使命 “即時反制所有威脅”

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

報告

根因分析報告，源頭追蹤、修補建議，確保未來不再發生

4

處理

協助客戶消除威脅，含刪除惡意程式、修改密碼建議、封鎖中繼站等

3

通知

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

2

分析

7x24蒐集與分析端點行為提供即時主動威脅獵捕服務

1



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？

無可比擬的精準

主動式威脅獵捕



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、最精準的警報確保企業安全。



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。

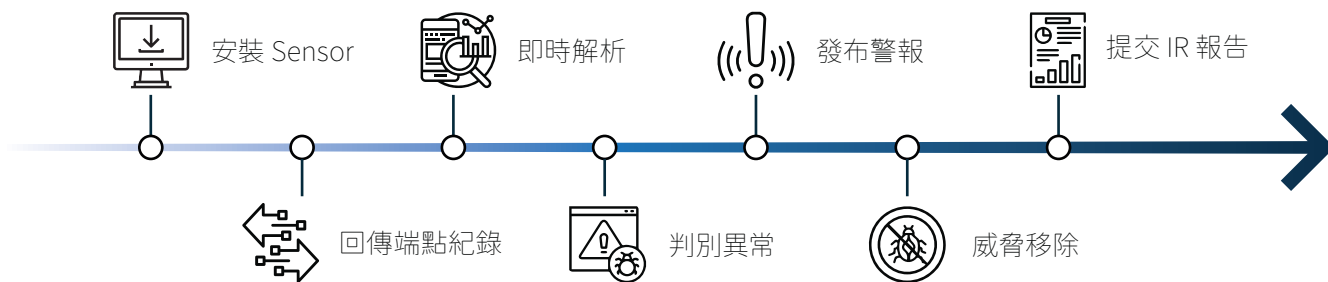


快速雲端原生部署

雲端原生設計最大化減少了部署投入的資源以降低營運成本，讓您在短短幾分鐘便可開始啟用保護。

全國唯一提供 7x24、無限 IR 的 MDR 服務廠商

服務流程



ITSEC MDR V.S SOC 優勢比較表

	ITSec MDR	SOC / SIEM
核心技術	Big Data + EDR	SIEM
處理方式	主動威脅獵捕與行為分析	被動依賴警報啟動調查
分析範圍	異常行為整體脈絡	圍繞警報本身
承諾服務	無限次數事件處理	通知及事件升級
服務效益	修復、根因分析	警報調查、關閉

事件處理流程-次數不限



系統基本需求

支援OS

- Windows 7+
- Windows Server 2008 R2+
- CentOS 7+
- Red Hat 7+
- Ubuntu 16.04+
- Debian 8+
- SUSE-SLES 12 SP3+

效能

- CPU 用量: 少於 1%
 - 頻寬需求: 平均每1000端點消耗 1Mb/s
- *估算基於 900 PC 及 100 Servers 的平均值

“ITSec MDR 交付的是成效，不是大量警報”

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

集時安全股份有限公司

☎ 02-2712-0855

@ sales@intimesec.com

📍 台北市信義區松山路130號7樓



intimesec.com