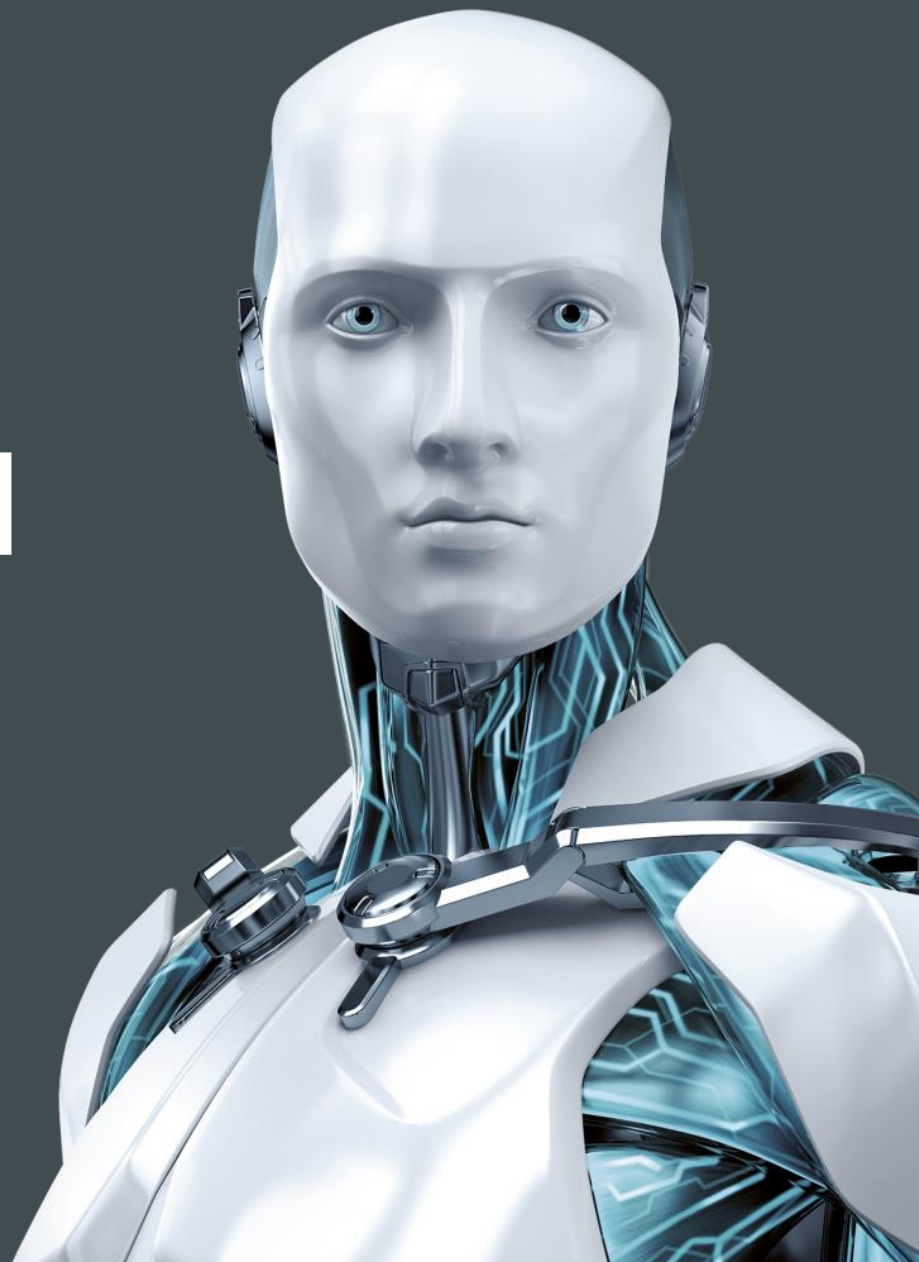
台灣二版簡介

Version 2 Limited 是亞洲其中一間最有活力的 **IT** 公司，公司發展及代理各種不同的互聯網、資訊科技、多媒體產品，當中包括通訊系統、保安、網絡、多媒體及消費市場產品。

透過公司龐大的網絡、銷售點、分銷商及合作伙伴，**Version 2 Limited** 提供廣被市場讚賞的產品及服務。**Version 2 Limited** 的銷售網絡包括香港、中國、台灣、新加坡、澳門等地區，客戶來自各行各業，包括全球 **1000** 大跨國企業、上市公司、公用機構、政府部門、無數成功的中小企及來自亞洲各城市的消費市場客戶。

V2 Version 2 | 二版
www.version-2.com

ESET PROTECT Cloud



ENJOY SAFER TECHNOLOGY™

使用ESET PROTECT Cloud先決條件

詳細資訊請依官網為主

- 擁有ESET Business Account 帳號。
- 擁有ESET PROTECT Cloud 之授權。
- 必須在網路防火牆中允許特定網域及連接埠【說明連結】

如何建立ESET PROTECT Cloud

詳細資訊請依官網為主

1. 登入 ESET Business Account
2. 點擊【**授權**】→【**輸入授權金鑰**】
3. 輸入【**您的專屬金鑰**】→【**新增授權**】
4. **授權登記之 mail 將會收取驗證信**　(確保欲管理授權之身份)
5. 至【**儀表板**】→【**啟動ESET PROTECT Cloud**】
6. 閱讀【**使用條款**】→選擇【**伺服器的位置（無法變更）**】→等待數分鐘
7. 完成後便進入ESET PROTECT Cloud Web Console

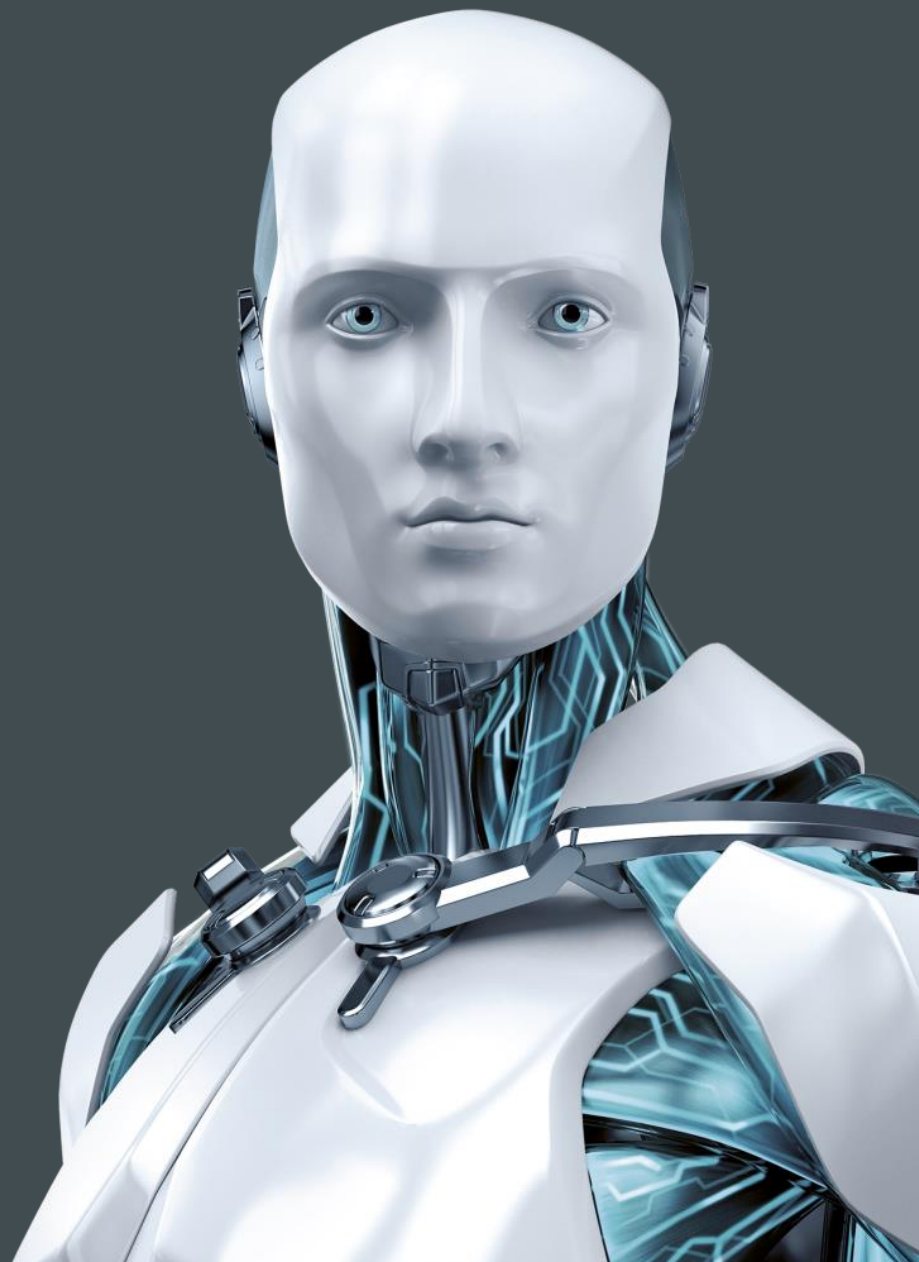
PROTECT V.S PROTECT CLOUD

雲端版中控台與中控版的差異

詳細資訊請依官網為主

	PROTECT	PROTECT CLOUD
主機	在實體或虛擬化環境上執行	在ESET維護的雲端環境中執行
可管理的裝置限制	視伺服器硬體而定	50000部用戶端裝置
授權管理	有部分在PROTECT，有部分在EBA	完全由EBA控制
Agent 預設連線間隔	1 分鐘（可變）	10 分鐘（不可變）
憑證	使用者可自行建立	由ESET管理
適用產品方案	任一 ESET 企業版產品	ESET 雲端企業版方案
安裝程式	下載檔案	除了下載檔案外,可透過電子郵件傳送具有指向安裝程式的連結

ESET Inspect



ESET ENJOY SAFER TECHNOLOGY™

概述

- ESET 端點偵測與回應，是屬於 EDR 解決方案。
- 可以記錄及分析客戶端程式行為。
- 收集數據：何時執行、由誰執行、執行多久、誰被攻擊
- 建立規則來響應檢測的事件

運作

詳細資訊請依官網為主

ESET Inspect 需有專門收集事件的主機，端點上需安裝額外的代理程式，並與 ESET PROTECT 及其防毒軟體整合在一起。

- 完整可用的 EEI 架構下，會需要有**兩部主機**：
  - ESET PROTECT
  - ESET Inspect Server

- 受管理的電腦上需要裝有**ESET 端點防護軟體與代理程式**：
  - ESET Endpoint Antivirus、ESET Endpoint Security 或 ESET File Security
  - ESET Management Agent
  - ESET Inspect Connector

資安威脅偵測分析服務

資安法修法 EDR 入列

依110年8月23日頒布之「資通安全責任等級分級辦法」修正條文明定如下：

資通安全責任等級A級與B級之公務機關：

本辦法中華民國一百十年八月二十三日修正施行前已受核定者，

應於修正施行後二年內，完成【端點偵測及應變機制】導入作業，並持續維運及依主管機關指定之方式提交偵測資料。

Endpoint Detection and Response 是?

【端點偵測回應】

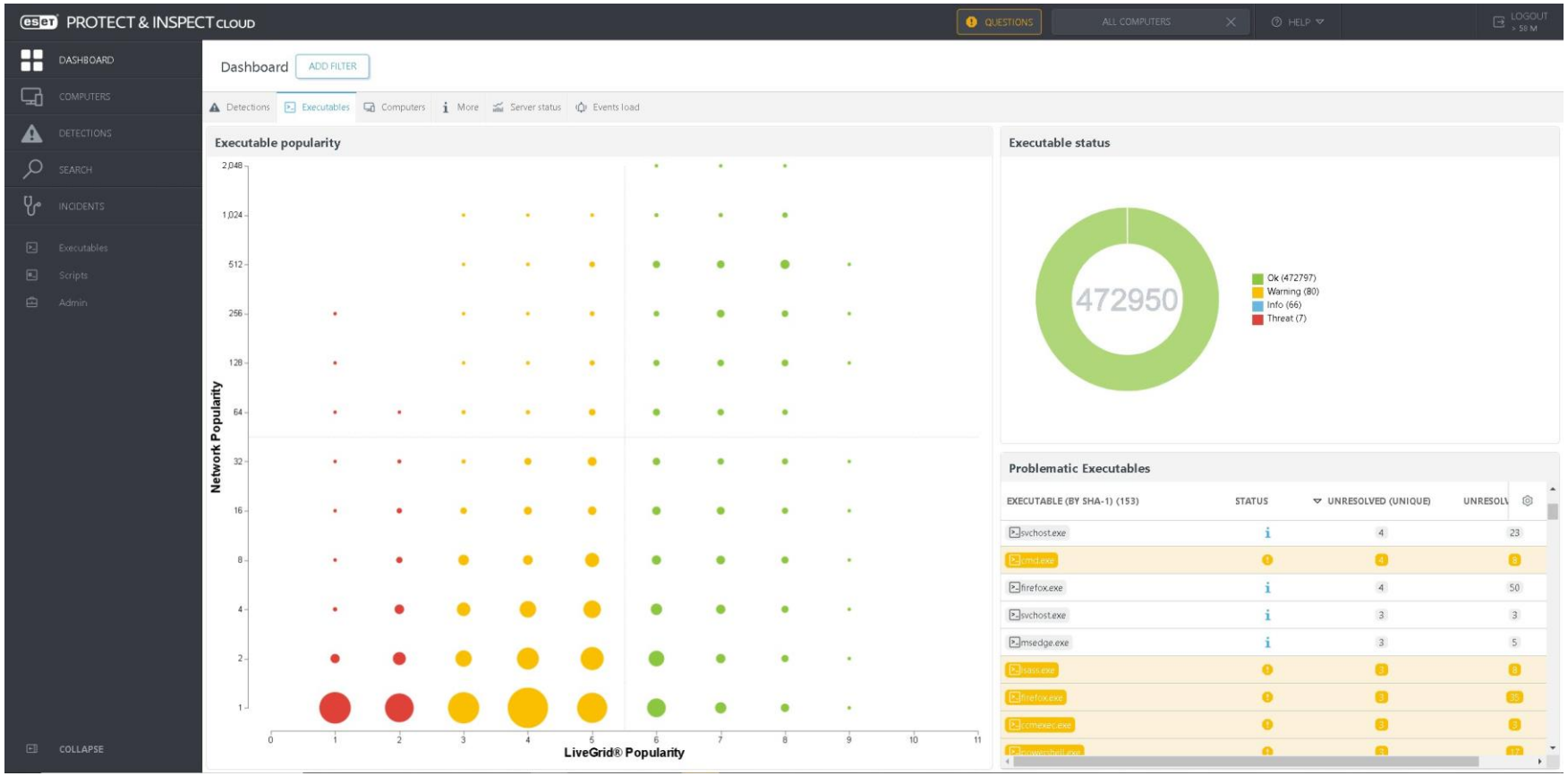
連接到網路的每台設備都代表來自 Internet 的威脅的潛在攻擊媒介，並且這些連接中的每一個都是通往您的資料的潛在Gateway；一般而言，EDR 解決方案從端點收集資料，使用它來識別潛在威脅，並提供有用的方法來調查和回應這些潛在威脅——現代解決方案甚至可以自動產出後續報告。

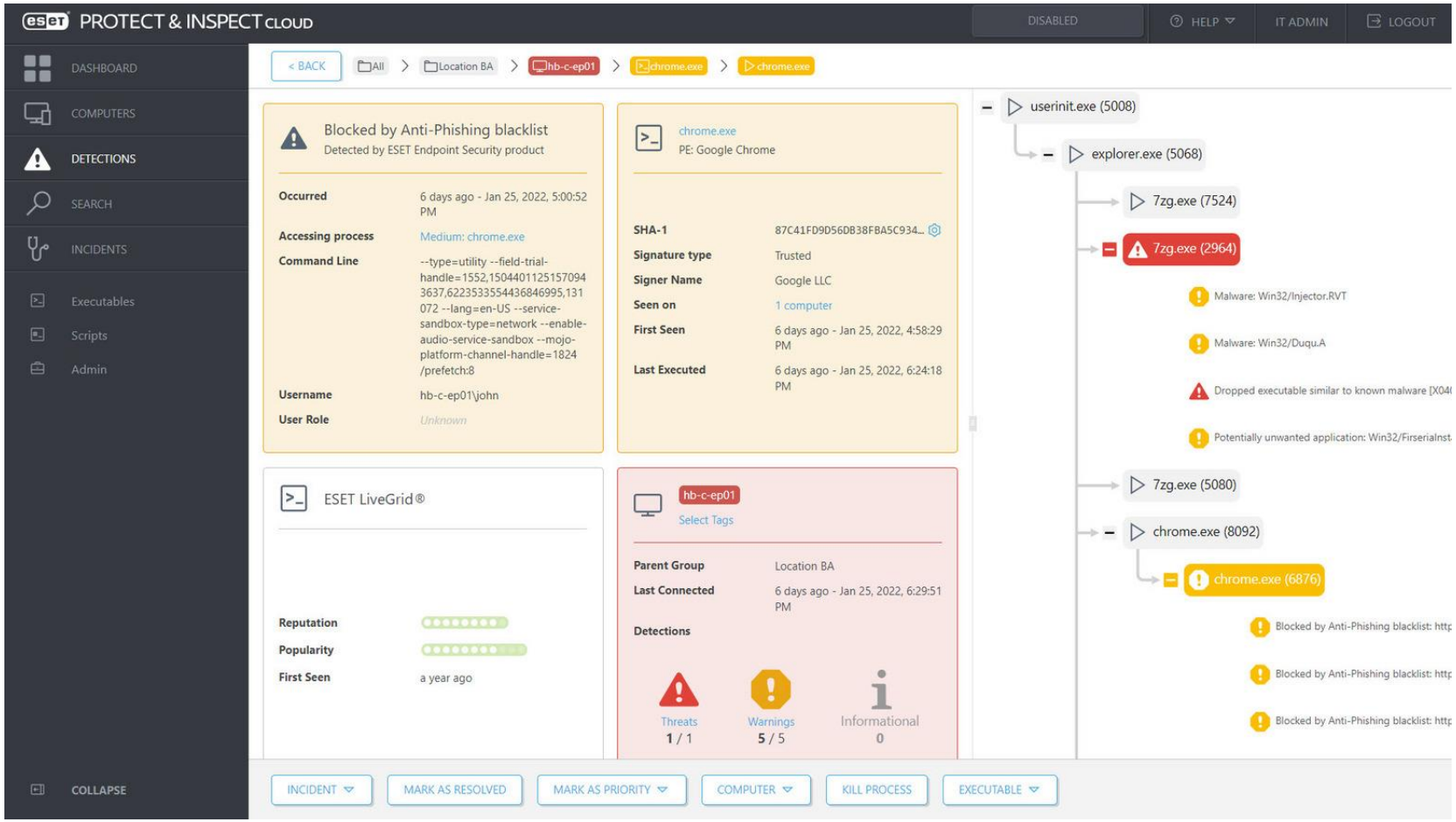
EDR 是?

範圍：端點和主機

意圖：端點/接入區域保護免受滲透、監控和緩解、漏洞評估、警報和回應

方法：惡意行為、攻擊指標 (IoA)、妥協指標 (IoC)、簽名(signatures)、機器學習(ML)





Managed Detection and Response 是?

【託管式偵測及回應】，這裡的重點不是技術，而是服務。作為 MDR 的一部分，客戶將他們的安全運營外包，並從全年、24 小時的可靠安全中受益。

安全供應商為他們的 MDR 客戶提供存取專門從事網路監控、事件分析和安全事件回應之安全分析師和工程師的權限。

MDR 是?

範圍：端點、主機、網路和設備間流量、應用程式

意圖：多個安全級別（網路、端點、應用程序）的可視性/透明度、在橫向級別偵測已知和未知威脅，包括所有組件、整體監控和緩解、漏洞評估、警報和回應、事件的簡化和整合，以及活動和有針對性的反應

方法：機器學習(ML)、攻擊指標 (IoA)、異常檢測、用戶行為、惡意行為、妥協指標 (IoC)

資安人力供給嚴重不足

網路安全系統分析師超搶手，光是今年第一季需求，每四家企業要搶1個求職者。

EDR, NDR, XDR 也需要不少資安人手

MDR 可以有效減輕人手負擔

UnderDefense

75 Security engineers

11 Certified Ethical Hackers

20 SOC analysts

11 Security Consultants

19 IT Engineers

320 Pentest projects

53K Systems protected

服務組合：

24x7x365 託管威脅回應

75 位安全工程師監視您的網路並保護您免受惡意攻擊者、勒索軟體和資料遺失

合規與 vCISO

快速輕鬆地獲得合規性， SOC2、ISO 27001、PCI DSS、GDPR ，我們對它們瞭如指掌，我們的 vCISO 將使其付諸實行

事件取證和資料洩露恢復

您需要快速獲得解答及恢復 – 我們能快速有效地調查、控制和補救關鍵安全事件

滲透測試

在駭客找到您的弱點之前。定期的健康檢查，對於成功的公司來說是必須的，我們是最擅長破壞安全的

三大好處：修復速度、卓越的 Python和自動化專業知識、非常划算

Version 2 台灣二版
www.version-2.com.tw

安全監控 / MDR 包

我們的安全監控是**定制的** 滿足每個公司的需求。我們將了解您的環境，並可以為您的安全團隊提供遠程增強功能。合作的基本模式有以下三種：

為您打造 SOC

當您決定與本地團隊一起構建 SOC，並且需要支持來為您的團隊選擇、計劃、實施和配置 SIEM/IR 工具並設置適當的流程時。我們就您的特定案例所需的最優化解決方案向您諮詢，維護您的 SIEM，為您的部署建立新的關聯

共同管理 SIEM/MDR/NTA

當您已經擁有或計劃購買 SIEM 但您想從投資中獲得答案和 ROI 但您無法聘請安全團隊或安全團隊不想在夜班期間工作，因此您需要擴展您的安全團隊與 UD 工程師一起配置、維護和監控

遠程 SOC 團隊

當您在內部擁有自己的 CIRT 團隊並且只需要我們的分析師進行監控和通知時。在這種情況下，我們可以在您自己的環境中工作或使用我們的 AWS 雲部署 Splunk 來監控事件並通知 CSIRT 團隊。您將收到調查結果報告，並與安全團隊保持持續溝通

UD MDR 訂閱入職流程（30 天）

1天	5天	8天	14天	2天
歡迎電子郵件	**啟動與規劃**	**連接和存取**	**服務配置**	**服務啟動**
• 介紹 • 入職表格請求 • 設置技術開始	• 技術啟動 • 審查技術文件 • 制定項目計劃和時間表 • 設置通訊渠道 • 定義需要建立的存取權限/憑據	• 建立新的客戶租戶 • 準備編譯 • 傳感器 • 通過 RMM 運送和部署傳感器 • 驗證和確認連接和訪問	• 配置和規範化i資料擷取 • 環境壓力測試 • 系統微調 • 誤報補救 • 自動化引擎 • 與客戶環境集成	• 定義升級程序和 IR 參與 • 啟動 “保護模式” • 服務集成驗證 • 服務期開始

商業考量：建構與購買

自己動手做：

24x7 支持需要

一位分析師 = USD 30-50K/YR

招聘= USD 3-5K / 每位員工

入職/培訓= USD 2-3K

聘請解決方案**工程師/管理員**= USD 40 - 60K/YR

人力資源 / 辦公室 / 管理= USD 60-80K / YR

設備/設備= USD 1.5-2K / 每個員工

購買**SIEM** =USD 50-100K/YR，
EDR = USD 45-75K/YR

估算持續存儲成本

實施經過驗證的威脅追蹤流程 + 輪班工作