

# 現代化之路：打造無塵室設備的 資安與運維監控神經中樞

基於 Wazuh 與 ELK 的整合性解決方案

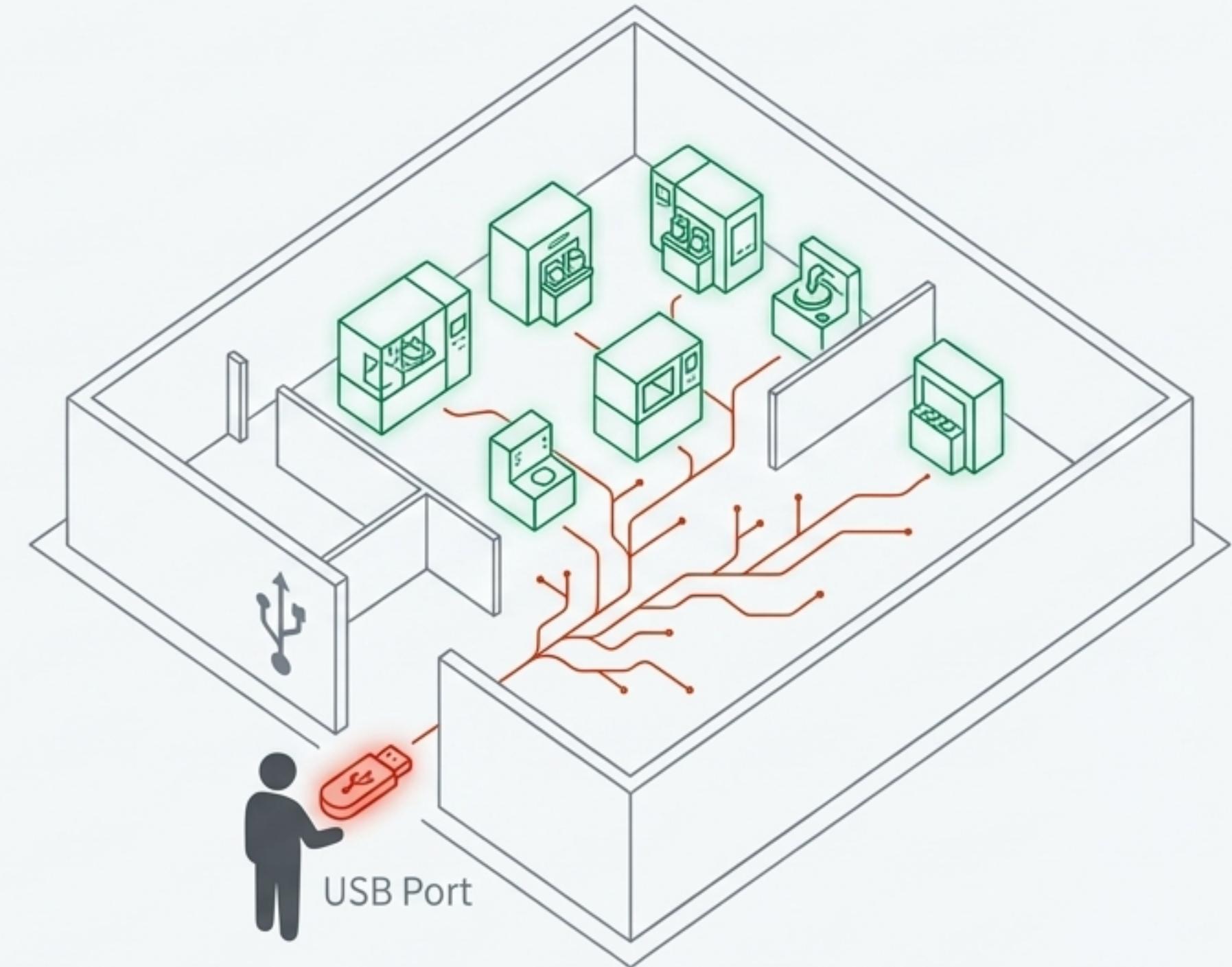


## 您最昂貴的資產，也是最脆弱的環節？

半導體製造的核心—昂貴的機台設備—多半運作在缺乏防護的舊版作業系統上。  
這些生產命脈正曝露於日益增長的資安與營運風險之中。

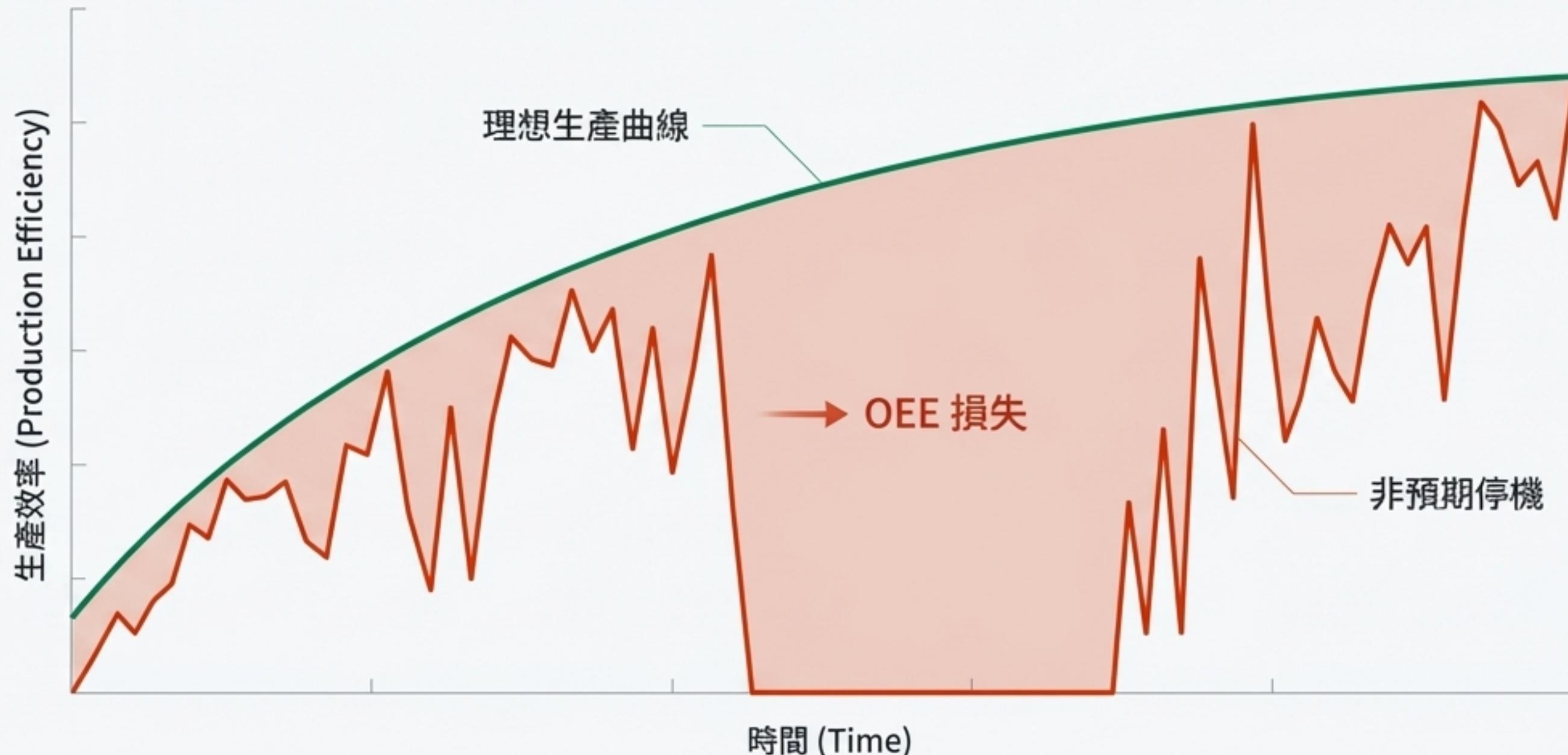
# 痛點一：資安盲區， USB 成為最大破口

- **封閉網路的迷思**：機台多處於封閉網路，但人員與 USB 設備的頻繁進出，使其成為病毒傳播的溫床。
- **過時的防護**：大量設備仍使用 Windows XP/7 等已停止支援的系統，無法更新病毒碼，形同不設防。
- **缺乏可視性**：無法即時偵測未經授權的設備接入或異常活動，潛在威脅在內部潛伏。



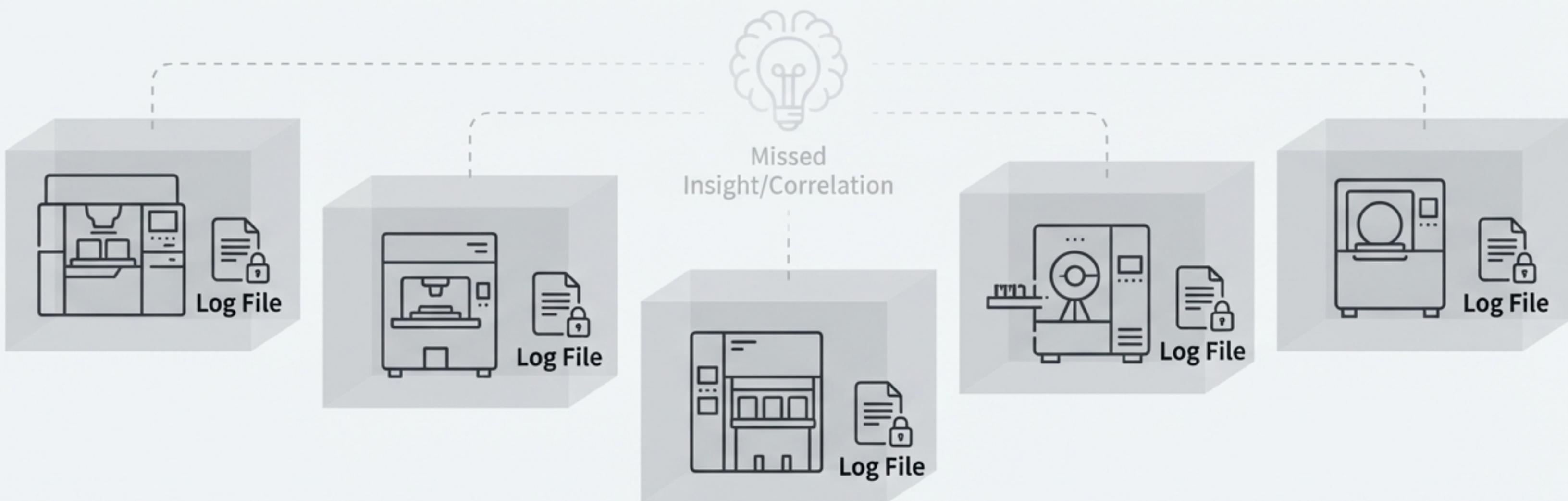
## 痛點二：運維被動，永遠在為停機救火

我們總在等待問題發生。等到機台因硬碟滿載、記憶體不足或程式崩潰導致「Down Tool」，工程師才介入處理。每一次的非預期停機，都在侵蝕 OEE。



## 痛點三：數據孤島，錯失洞察與預警的先機

每台機台的日誌（Log）都被鎖在各自的電腦中。沒有統一的平台，就無法進行關聯分析，也無法從海量數據中找出潛在故障的模式或資安事件的蛛絲馬跡。黃金數據變成了無用資訊。

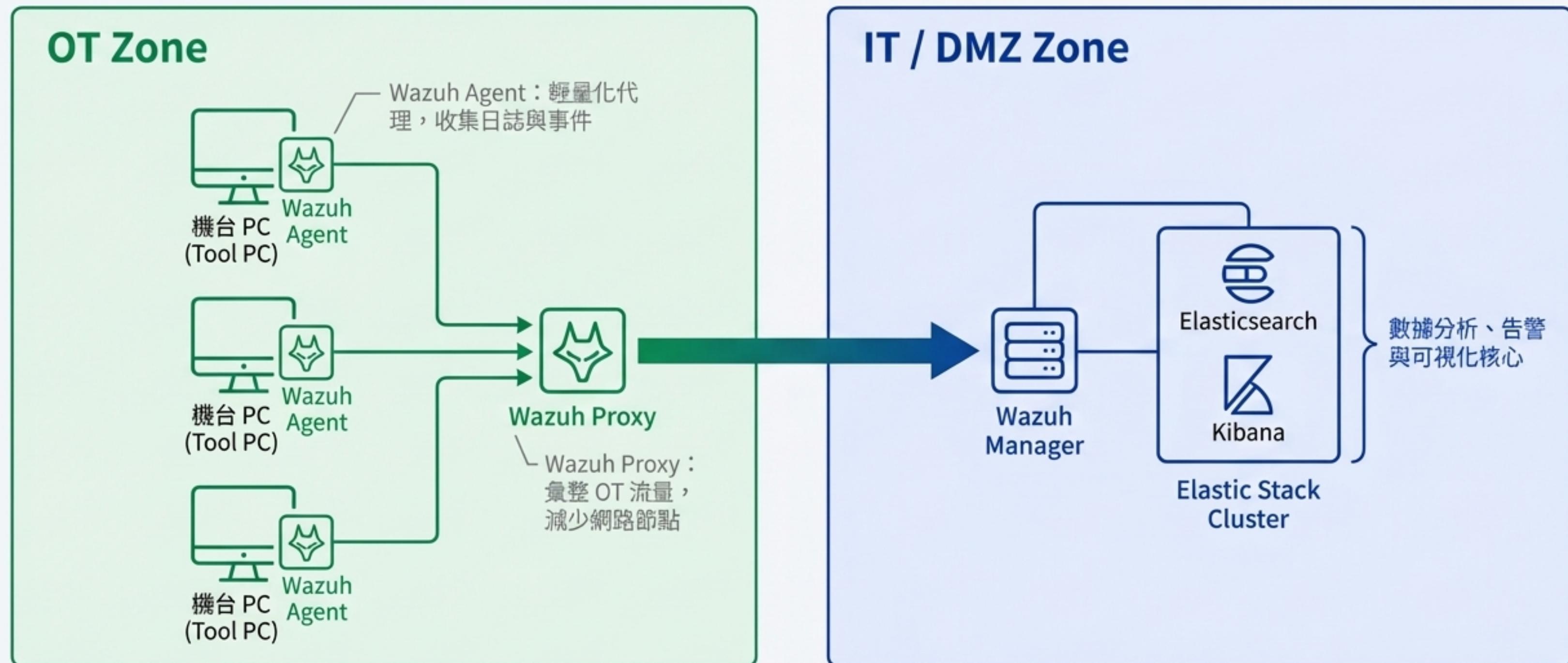


# 搭建一座橋樑：連接孤立的 OT 與智慧化的 IT



我們提出的不是單一的防毒或監控軟體，而是一個完整的「SecOps 橋樑」。它安全地從 OT 環境中收集關鍵數據，並在 IT 環境中進行集中的分析、可視化與告警，且不影響產線運作。

# 方案架構：安全、高效的數據採集與分析拓撲



# 關鍵功能一：USB 防護網，化被動為主動的邊界守門員

## 即時監控

系統即時監控所有 PnP（隨插即用）事件。

## 立即告警

當任何未經授權的 USB 設備插入機台時，立即觸發告警至戰情室，並詳細記錄該設備的 ID、廠商與產品資訊。



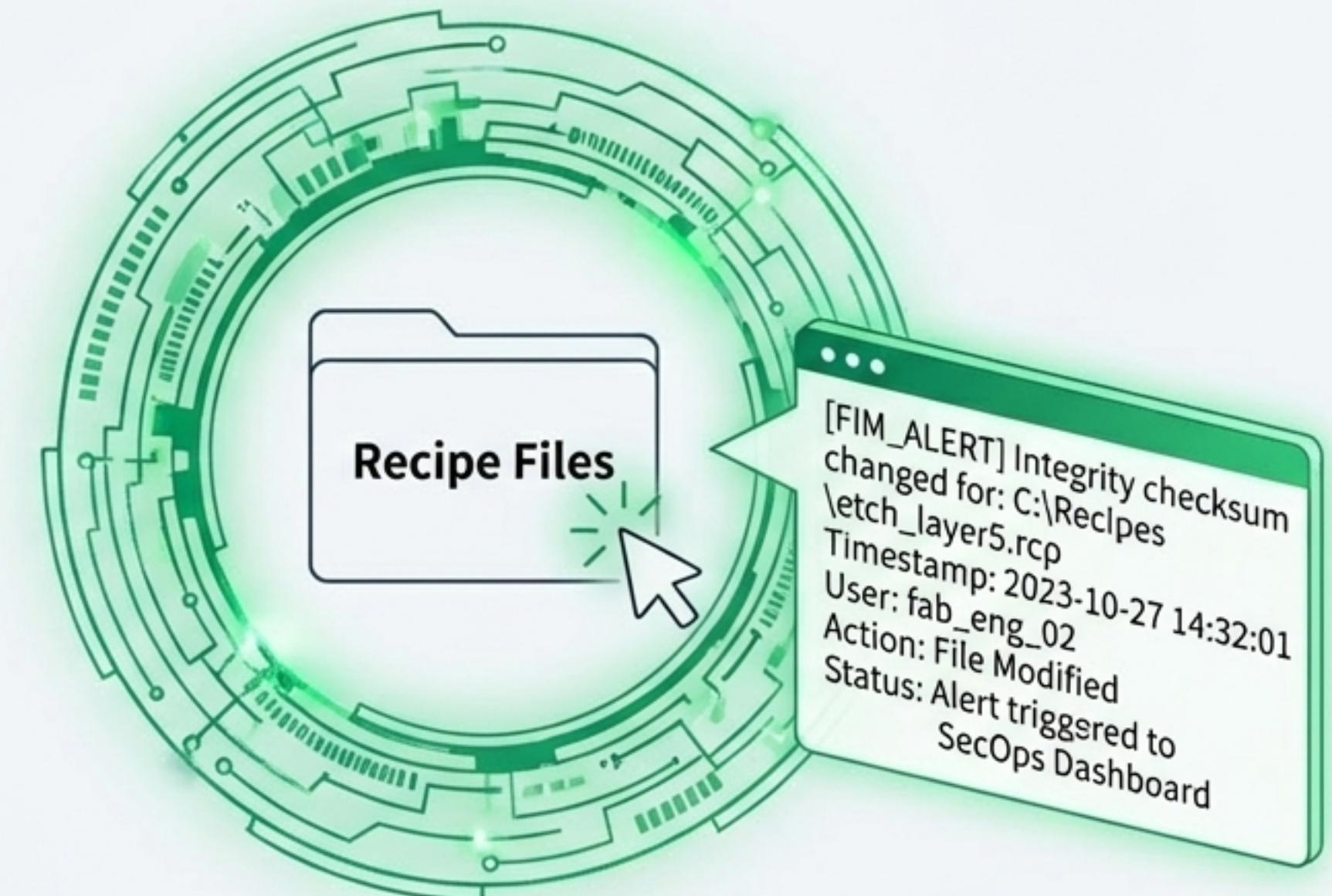
# 關鍵功能二：Recipe 守護者，確保製程參數 的絕對完整

## 檔案完整性監控 (FIM)

針對儲存製程參數的 Recipe 檔案夾與檔案，實施 24/7 的完整性監控。

## 滴水不漏的稽核

任何對 Recipe 的修改、刪除或權限變更操作，都會被即時記錄並發出告警。確保製程的穩定與一致性，滿足「Copy Exact」要求。



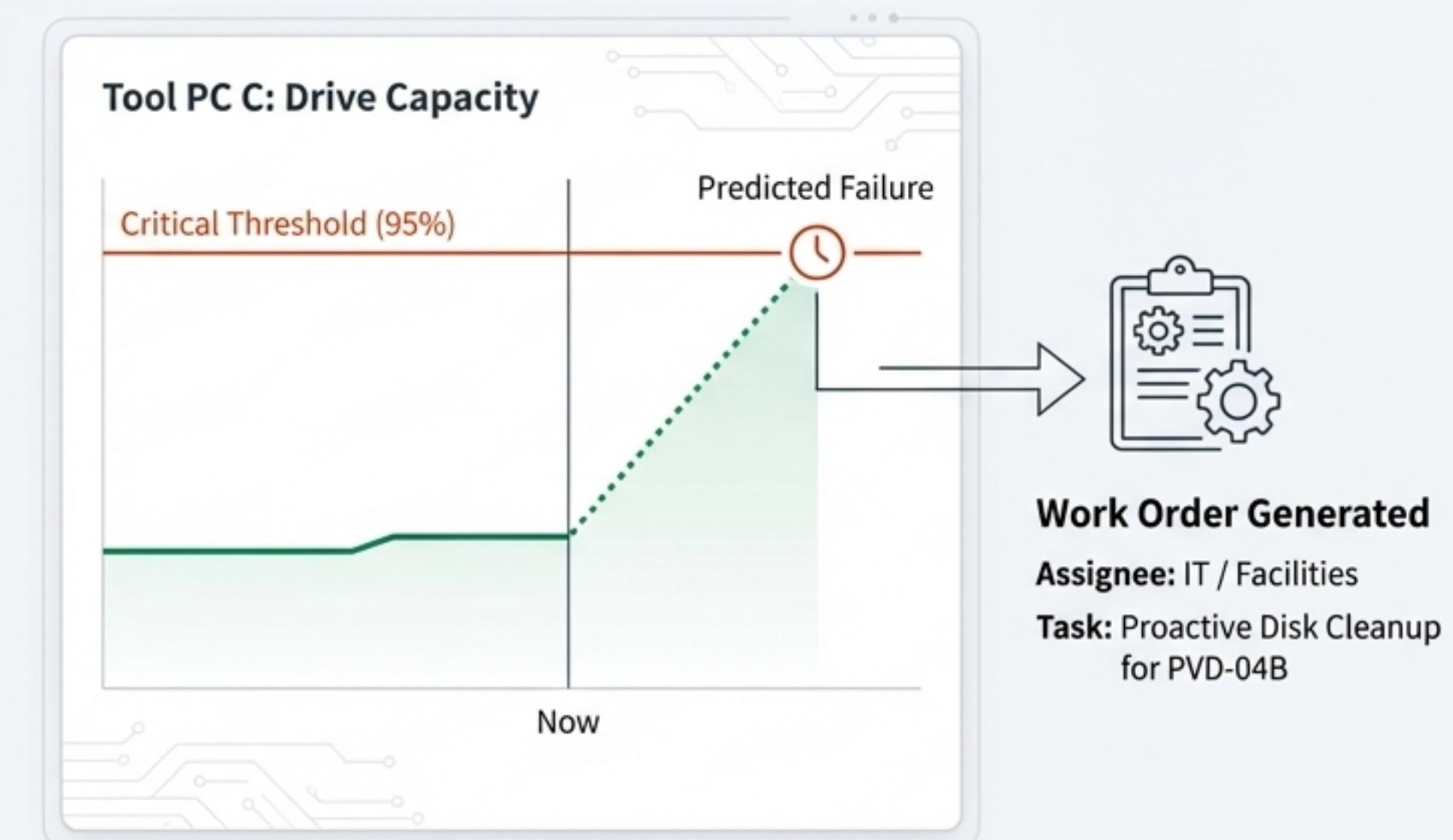
# 關鍵功能三：效能預警，從源頭終結非預期停機

## 健康狀態監控

持續監控機台 PC 的關鍵效能指標，包括 CPU 使用率、記憶體佔用、以及硬碟剩餘空間。

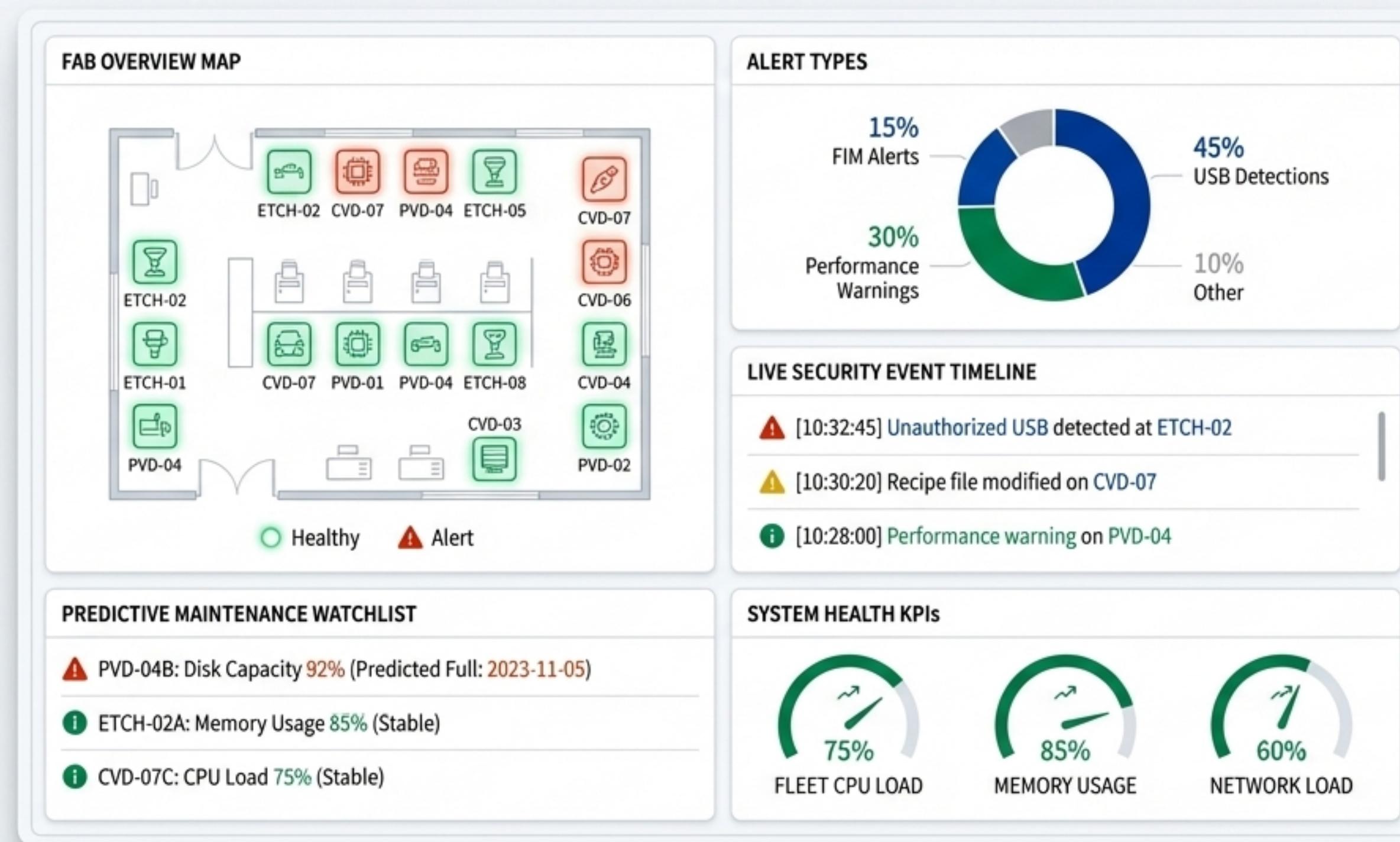
## 自動化預警範例

可設定規則，例如「當任一機台硬碟空間剩餘低於 5% 時，自動發送工單通知 IT 與廠務團隊進行預防性維護」。



# 成果：從各自為政到運籌帷幄的「單一戰情室」

透過 Kibana，所有機台的資安事件與運維數據被匯整至統一的儀表板。管理者能一目了然地掌握全廠動態，實現從被動反應到主動預測的根本轉變。



# 方案的商業效益：更低風險、更高效率、更優成本



## 1. 顯著降低風險

- 有效減少因 USB 病毒或惡意操作導致的產線停機事件。
- 自動產出稽核日誌，滿足 ISO 27001 與 SEMI E187 等半導體資安合規要求。



## 2. 全面提升 OEE

- 透過效能預警機制，成功將「非預期停機」轉化為「計劃性維護」。
- FIM 確保製程穩定，降低因參數錯誤造成的良率損失。



## 3. 實現絕佳成本效益

- 採用業界驗證的開源架構，大幅降低軟體授權與維護費用。
- 具備高度客製化彈性，避免被單一廠商鎖定。

# 這不僅是資安強化，更是無塵室數位轉型的基石

在不淘汰昂貴機台的前提下，本方案融合了資安防禦與智慧運維 (SecOps)。它是打通數據壁壘、實現預測性維護、並邁向工業 4.0 智慧製造的最佳、也最務實的第一步。

