端點偵測及應變□EDR□服務

端點偵測及應變機制(Endpoint Detection and Response, 簡稱EDR)主要目的為偵測端點系統上異常活動，以期能及早發現駭客活動跡象，降低後續可能引發之資安風險。

本服務為配合本校資通安全責任等級C升B計畫中，達成B級機關應辦事項技術面之「端點偵測及應變機制」要求建置，此服務已完成測試導入，於113年12月正式上線。

端點偵測及應變服務說明

1. 主要協助檢測、識別和回應可能的威脅，特別是端點□PC□Server□隨時監控網路與端點資料，減少可能遭遇的威脅（勒索軟體、進階持續性攻擊□APT□□等。
2. 提供即時監控□log 收集、威脅檢測和分析功能；以協助資安人員快速追蹤端點上的異常活動，並對潛在威脅做出快速回應。
3. 委託專業資安廠商提供 7*24 監控、事件分析、提攻防護建議和可行的異常解決方案。

服務申請注意事項

1. 因目前授權數有限，優先以配合計通中心進行資訊系統分類分級作業之系統管理員申請，請系統管理員透過 email 向服務聯絡人提出申請。
2. 如授權數尚有餘裕可供對外提供服務網站申請，請單位網管向服務聯絡人洽詢與申請。
3. 此服務需於系統上安裝 Agent 軟體，申請時提供相關下載連結，目前支援的作業系統如下：
    - Windows (Windows 7 / Windows 10 / Windows Server 2008 R2 or above)
    - Linux (Ubuntu / Debian / CentOS / Fedora)
    - macOS (macOS 10.15 / macOS Big Sur 11.1)
4. 可能需調整既有的防火牆規則，允許與本服務之間的通訊連線。

服務聯絡人：網路系統組 施先生，校內分機 31134，郵件信箱□yucshih @ mx.nthu.edu.tw