**會議名稱：達和環保SIEM雙周會**

日期： 2025-02-18

時間： 10:00 - 12:00

地點： 達和環保6F會議室

主持人： Barry

記錄人： Barry

出席人員：達和環保Joy、達和環保Harry、明竑科技Barry、聯達資訊Lance

缺席人員： 無

**會議議程**

1. 開場與確認議程

2. 上次會議回顧與追蹤事項

- 第一次會議(啟動會議)故無上次會議回顧與追蹤事項。

3. 新議題討論

- **議題 1**： SIEM建置時程確認。

- 討論內容： SIEM建置時程第一階段需在2025-03-31完成，包含設備收容及報告產出。後續有其他收容設備或需要優化則在安排第二階段執行。

- 決議事項： 第一階段需在2025-03-31完成，並安排雙周會確認進度。

- 負責人： Barry、Lance、Harry

- 完成期限： 2025-03-31

**- 議題 2： 確認收容設備清單**

- 討論內容： 將現有地端伺服器Log納入SIEM並說明需要在Server上安裝Agent。

- 決議事項： ，請Harry彙整伺服器清單(含作業系統版本、Service)，Lance提供Agnet及安裝文件。

- 負責人： Harry、Lance

- 完成期限： 2025-02-20

**議題 3： 防火牆flow設定。**

- 討論內容： 確認防火牆Policy開啟，將目前現有防火牆flow收容到SIEM。

- 決議事項： 在2025-02-24完成。

- 負責人： Barry、Lance、Harry

- 完成期限： 2025-02-24

**議題 4： 防火牆失聯問題。**

- 討論內容： 約有11台防火牆收容後不定時跳出ICMP Fail。

- 決議事項：持續觀察並查找問題。

- 負責人： Barry、Lance、Harry

- 完成期限： 2025-02-26

4. 其他事項

- 雲端服務也要納入SIEM，請管理員駱哥參與下次會議。

5. 下次會議安排

- 日期與時間： 2025-03-04

- 地點或方式： 達和6樓會議室