(07)專案管理 - 專案資訊 #982

SIEM 安全資訊與事件管理平台 -設備收容

2025-02-19 15:22 - 益利 周

狀態:	Resolved-解決	**開始日期:**	2025-01-01
優先權:	Normal	**完成日期:**	2025-03-31
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	0:00 小時
版本:		**耗用工時:**	40:00 小時

概述

SIEM 平台 https://192.168.4.181/

歷史

#1 - 2025-02-19 15:27 - 益利 周

建置規劃
一月　網路設備收容。　　已加入各地防火牆設備。
二月　伺服器.地端.雲端其他設備收容。　　正進行中。
三月　設備,及伺服器等 資料產出及狀態通知。

#2 - 2025-02-19 15:31 - 益利 周

- 檔案 達和環保SIEM雙周會_第一次會議20250218.docx 已新增

排定 雙周會議 檢討進度
2/18, 3/4, 3/18, 4/1

#3 - 2025-02-21 13:47 - 益利 周

- 完成日期 設定為 2025-03-31

- 狀態 從 New-新增 變更為 In process-進行中

- 開始日期 從 2025-02-19 變更為 2025-01-01

- 完成百分比 從 0 變更為 30

一月 已將 全省防火牆 設定進 SIEM 內.

本月 持續將 其他硬體設備及伺服器 加入 SIEM 監控中.

#4 - 2025-03-10 09:35 - 益利 周

- 完成百分比 從 30 變更為 40

3/4 SIEM 雙周會

會議名稱：達和環保SIEM雙周會
日期： 2025-03-04
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：達和環保駱哥、達和環保Harry、明竑科技Barry、明竑科技Ivan、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
- FW flow設定完成。
- Server log收容清單Harry已經提供。
- FW 失聯問題持續觀察。
3. 新議題討論
- 議題 1： Server log清單討論。
- 討論內容： 針對Server收容清單再清楚標上每台Server有跑那些service?例如:Server上有跑IIS、SQL等則要標示出來。
- 決議事項：先針對單一service的Server進行log收容，。
- 負責人： Ivan、Lance、Harry

- 完成期限： 2025-03-07

- 議題 2： 確認教育訓練時間
  - 討論內容： 討論教育訓練時間。
  - 決議事項： ，目前進度3月底完成設定，教育訓練暫定安排在4月。
  - 負責人： Barry
  - 完成期限： 2025-03-18

議題 3： Server log設定。
- 討論內容：確認Server清單及services。
- 決議事項：針對單一台Server上只有單一Service的主機優先設定，安排3/7 星期五過去達和設定。
- 負責人： Ivan、Lance
- 完成期限：2025-03-07

議題 4： NP 帳號整合LDAP設定。
- 討論內容：提供相關技術文件給Harry參考。
- 決議事項：另外安排時間到現場設定。
- 負責人： Ivan、Lance
- 完成期限：2025-03-07

4. 其他事項
- 無
5. 下次會議安排
- 日期與時間： 2025-03-18
- 地點或方式： 達和6樓會議室

#5 - 2025-03-10 09:58 - 益利 周

- 完成百分比 從 40 變更為 50

3/7
AD 帳號設定完成
目前 IT 管理人員 可經由 AD 帳號登入 SIEM 管理
https://siem.tahoho.com.tw/

授權人員 (以下人員之管理帳號)
廖毓銘、駱正達、周益利、胡志鴻、楊政益、曾仰正、林谷穎、謝尚谷、賴志明、吳明哲、陳君華、吳振杰、黃弘政、陳宗沛
。

地端及雲端設備 9台 Windows Server 記錄收容。

#6 - 2025-03-24 10:10 - 益利 周

- 檔案 達和環保SIEM雙周會_第三次會議20250318.docx 已新增

- 完成百分比 從 50 變更為 70

SIEM 平台 建置雙週討論

1.LDAP 認證 - 設定完成.已授權予 IT 管理人員可登入使用.
2.Server Log 設定完成 (Windows Server Log)

新議題

1.監控設備 離線告警.
2.Dashboard 設定
3.Report格式

詳見會議記錄

#7 - 2025-03-24 10:17 - 益利 周

- 檔案 clipboard-202503241014-cen19.png 已新增

- 檔案 clipboard-202503241015-82wgk.png 已新增

- 檔案 clipboard-202503241016-xggmt.png 已新增

1.網站 SSL 設定

clipboard-202503241014-cen19.png
2.Logo 更換

clipboard-202503241015-82wgk.png

clipboard-202503241016-xggmt.png

#8 - 2025-04-02 15:52 - 益利 周

- 完成百分比 從 70 變更為 80

會議名稱：達和環保SIEM雙周會
日期： 2025-04-01
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 Harry、達和環保 正達 、Barry
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
- 部分設備ICMP Fail產生告警，已經處理完成。
- Dashboard設定和Report設定未完成。
- NP版本更新到3/13最新版本，確認ICMP及flow正常。

3. 新議題討論
- 議題 1： 部分設備離線。
- 討論內容： 調整會議時間。
- 決議事項：維持雙周會但會議開始時間改成10:30。
- 負責人： Barry
- 完成期限： 2025-04-01

- 議題 2：Dashboard設定
  - **討論內容： 討論Dashboard畫面。**
  - **決議事項：設定Dashboard畫面供達和參考。**
  - **負責人： Lance**
  - **完成期限： 2025-04-14**

議題 3： Report格式討論。
- 討論內容：討論Report格式。
- 決議事項：先提供其他客戶Report格式並產出Report供達和參考。
- 負責人： Lance
- 完成期限：2025-04-01

議題 4： 密碼錯誤log訊息。
- 討論內容：log一直出現使用者密碼錯誤訊息。
- 決議事項：先查看log，找出位於台北的使用者，查看使用者桌機及Server。
- 負責人： Barry、Harry
- 完成期限：2025-04-01

議題 5： HR系統監控。
- 討論內容：HR反映HR系統常離線，HR系統採用Clinet Server架構，DB在TAHO-HR、Web在TAHO-SMHR。
- 決議事項：。調整設定，確定是否可以納入監控?
- 負責人： Lance
- 完成期限：2025-04-014

議題 6：Core SW SNMP離線。
- 討論內容：從NP上測試SNMP功能無法成功，研判是SW端SNMP設定出問題。
- 決議事項：提供型號及韌體版本，確認SW是否有支援及如何設定。
- 負責人： Barry
- 完成期限：2025-04-14

議題 7： NP備份計畫。
- 討論內容：不清楚NP備份設定。
- 決議事項：提出備份建議，並說明備份功能。
- 負責人： Lance
- 完成期限：2025-04-14

4. 其他事項
- 無

5. 下次會議安排
- 日期與時間： 2025-04-15
- 地點或方式： 達和6樓會議室

#9 - 2025-04-21 15:11 - 益利 周

- 檔案 clipboard-202504211502-2cgom.png 已新增

- 檔案 clipboard-202504211503-civxm.png 已新增

- 檔案 clipboard-202504211505-ewtp7.png 已新增

- 檔案 clipboard-202504211506-t5wuj.png 已新增

- 主旨 從 SIEM 安全資訊與事件管理平台 變更為 SIEM 安全資訊與事件管理平台 -設備收容

- 狀態 從 In process-進行中 變更為 Resolved-解決

- 完成百分比 從 80 變更為 100

完成 SIEM 設備記錄 收容
Azure 8台
clipboard-202504211502-2cgom.png
達和 30台
clipboard-202504211503-civxm.png
上水 15台
clipboard-202504211505-ewtp7.png
達清 3台
clipboard-202504211506-t5wuj.png

檔案

達和環保SIEM雙周會_第一次會議20250218.docx	**28.4 KB**	**2025-02-19**	**益利 周**
達和環保SIEM雙周會_第三次會議20250318.docx	**28.2 KB**	**2025-03-24**	**益利 周**
clipboard-202503241014-cen19.png	**391 KB**	**2025-03-24**	**益利 周**
clipboard-202503241015-82wgk.png	**391 KB**	**2025-03-24**	**益利 周**
clipboard-202503241016-xggmt.png	**116 KB**	**2025-03-24**	**益利 周**
clipboard-202504211502-2cgom.png	**15.3 KB**	**2025-04-21**	**益利 周**
clipboard-202504211503-civxm.png	**65.6 KB**	**2025-04-21**	**益利 周**
clipboard-202504211505-ewtp7.png	**32.4 KB**	**2025-04-21**	**益利 周**
clipboard-202504211506-t5wuj.png	**6.81 KB**	**2025-04-21**	**益利 周**