透過GPT類大型語言模型整合安全運營中心的資安微服務架構

專題編號:113-CSIE-S030
執行期限:112年第1學期至113年第1學期
指導教授:張世豪
專題參與人員: 110590025 卓佑霖
110590058 林秉憲
110590060 林正峰
110590061 陳識勛

1、 摘要

隨著無人搬運車(Automated Guided Vehicle, AGV)技術的發展，本研究探討將AGV引入資訊安全領域，並建立一個強化的資訊安全運營中心(SOC)模型。本研究主要關注於整合安全資訊與事件管理(Security Information and Event Management, SIEM)、安全自動化與響應(Security Orchestration, Automation, and Response, SOAR)技術，以及人工智慧機制，提升對於惡意攻擊的偵測、分析與應對能力。

其次，本研究考慮到不同層次和複雜度的攻擊可能存在，我們也會利用大型語言模型(LLM)作為AGV產生的事件日誌的整理工具，分析及過濾不必要的資訊，將難以閱讀的日誌轉化成更加可視化的報表即時辨識並分類不同類型的攻擊並通知資安防護人員。

關鍵詞:AGV、SIEM、SOAR、LLM

2、 緣由與目的

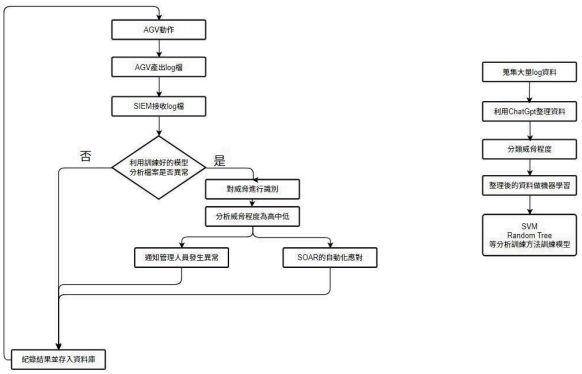
在現今快速發展的現代社會中，自動引導車輛(AGV)正以其獨特的技術優勢和廣泛應用的方式，助力我們走向更智慧、高效的未來。這種無人操控的新型態載具在各行各業發揮著關鍵作用，然而，隨著AGV應用變得更加廣泛，同時也必須面臨著一系列資訊安全挑戰，因為AGV的自主性和連接性使其面臨潛在的風險，可能受到不法分子的攻擊。首先，駭客可能試圖入侵AGV的控制系統，從而破壞其正常運行，為了防止這樣的惡意攻擊事件，市面上已經有不少關於這種攻擊事件的處理手段，SIEM與SOAR就是最好的例子，但是絕大多數的處理手段都屬於被動偵測，所以我們計畫設計一個SOC，整合SIEM與SOAR，並引入LLM作為分析預測工具，以縮短偵測錯誤到做出防護措施的時間。

3、 研究報告內容

通過整合SIEM技術，實現對AGV運行過程中產生的事件和日誌的即時收集、管理和分析。SOAR技術進一步引入自動化響應機制，提高SOC的應對效率，尤其是在攻擊發生時的快速反應。過程中我們將會導入大型語言模型提升偵測攻擊時的速度與精準度，從而減小被攻擊到預防的時間，更加有效率的進一步防止威脅的擴散。

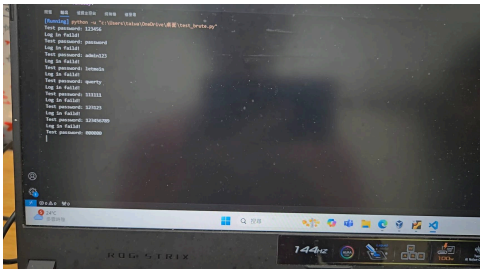
在AGV上建置Wazuh開源監控平台對其進行安全監控與威脅應對，其所整合的EDR與SIEM功能，可以供我們收集、分析和應對安全事件，提高AGV運行時的安全性。我們計畫目前已經擁有 Wazuh 的警示與Log 檔，透過使用Wazuh的log收集功能，實時監控AGV在運作時產生的log，通過Wazuh Agent代理程式將檔案傳送至Wazuh Server。並且讓Wazuh Server與SOAR工具Shuffle連結，觸發workflow串接ChatGPT API做資料過濾及處理，最後

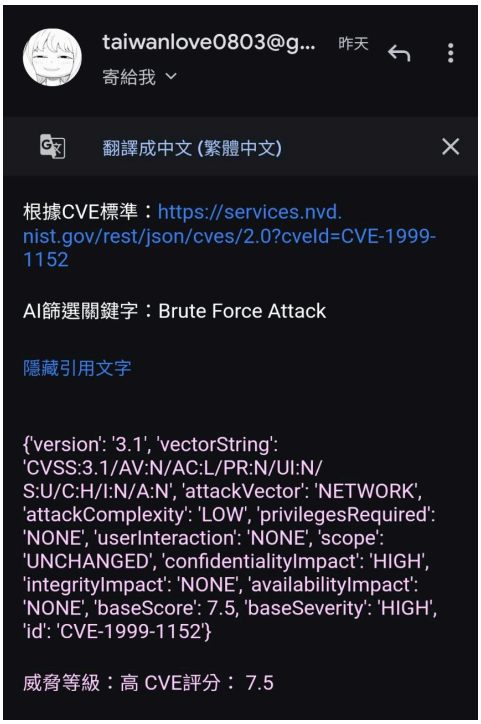
將告警資訊利用Email告知維護人員。



圖一:車聯網惡意程式偵測系統流程圖

4、 實驗結果





5、 結論

本研究計畫旨在建立一個基於軟體定義車聯網的安全監控系統，透過整合SIEM和SOAR技術，提升無人搬運車（AGV）的資訊安全。實驗結果顯示，系統能夠實時監控並自動檢測安全事件，降低安全威脅風險，同時提高運行效率，此外，系統的泛用性使得我們能夠迅速調整和應用於其他AGV，實驗結果顯示該系統能有效降低安全風險，提高運行效率。

參考文獻

[1] J.B.Kenney,"Dedicated short-range communications (DSRC) standards in the United States, "*Proceedings of the IEEE,* vol. 99, no. 7, pp. 1162-1182, 2011.

[2] L. Qiu, W.-J. Hsu, S.-Y. Huang, and H. Wang, "Scheduling and routing algorithms for AGVs: a survey," *International Journal of Production Research,* vol. 40, no. 3, pp. 745-760, 2002.

[3] F. Taghaboni-Dutta and J.M.A.Tanchoco, "Comparison of dynamic routeing techniques for automated guided vehicle system," *International Journal of Production Research,* vol. 33, no. 10, pp. 2653-2669, 1995.

[4] K. Demertzis, P. Kikiras, N. Tziritas, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: network flow forensics using cybersecurity intelligence," *Big data and cognitive computing,* vol. 2, no. 4, p. 35, 2018.

[5] M. Ahmid and O. Kazar, "A comprehensive review of the internet of things security," *Journal of Applied Security Research,* vol. 18, no. 3, pp. 289-305, 2023.