

1. Introduction

This project outlined the implementation and evaluation of automation within the Microsoft Sentinel Security Information and Event Management (SIEM) platform in a real-world environment. As technology becomes more sophisticated, cyber security efforts must respond to the current network requirements.

Digital Health Care Wales (DHCW) is a health authority of NHS Wales, which has an all-Wales purpose of managing the Welsh healthcare network and systems. DHCW, and many of its projects, are a response to Welsh Assembly Government's Digital and Data Strategy for Health and Social Care in Wales[2]. The Welsh Assembly Government's Cyber Action Plan[3] highlights the requirement for all public bodies, including DHCW, to implement cyber resilience into service delivery.

This project aims to explore automation within Microsoft sentinel within DHCW, looking at automating routine responses and reducing alert fatigue. The project provides a review of the most recent available literature and outlines steps taken to explore integration within the NHS Wales network and infrastructure.

2. Aims & Objectives

The aim is to:
Implement and evaluate automation in Microsoft Sentinel to improve detection accuracy and reduce the response time in real world scenarios.

The objectives are:

1. Review current SIEM automation practices to identify limitations and best practices.
2. Apply a suitable research methodology with a clear project plan.
3. Design and build a mock Sentinel automation workflow using Logic Apps.
4. Test performance with simulated incidents, measuring accuracy, speed, and reliability.
5. Analyse results and recommend improvements for future SIEM automation.

3. Research

- Conducted a systematic literature review using the PRISMA framework to identify best practices, challenges, and opportunities in SIEM automation.
- Reviewed 40 sources on automation, detection accuracy, alert fatigue, and hybrid human–AI workflows.
- Applied a pragmatic, deductive approach using the Research Onion to guide design and evaluation.
- Used a design-based case study strategy focused on Microsoft Sentinel and Logic Apps within the DHCW context.
- Developed and tested a prototype workflow with simulated incidents to evaluate detection accuracy, response time, and reliability.

4. Design and Implementation

Built an automation workflow in Microsoft Sentinel using Logic Apps to enrich high-severity alerts with GeoIP (geographical internet protocol) data.

Workflow stages: trigger on high-severity alerts → filter irrelevant events → extract source IP → run GeoIP lookup → add formatted location data to the incident comment.

Chose Sentinel for existing NHS Wales deployment and Logic Apps for seamless integration without heavy custom coding.

Tested with simulated alerts every 5 minutes over 3 days to validate reliability, accuracy, and repeatability.

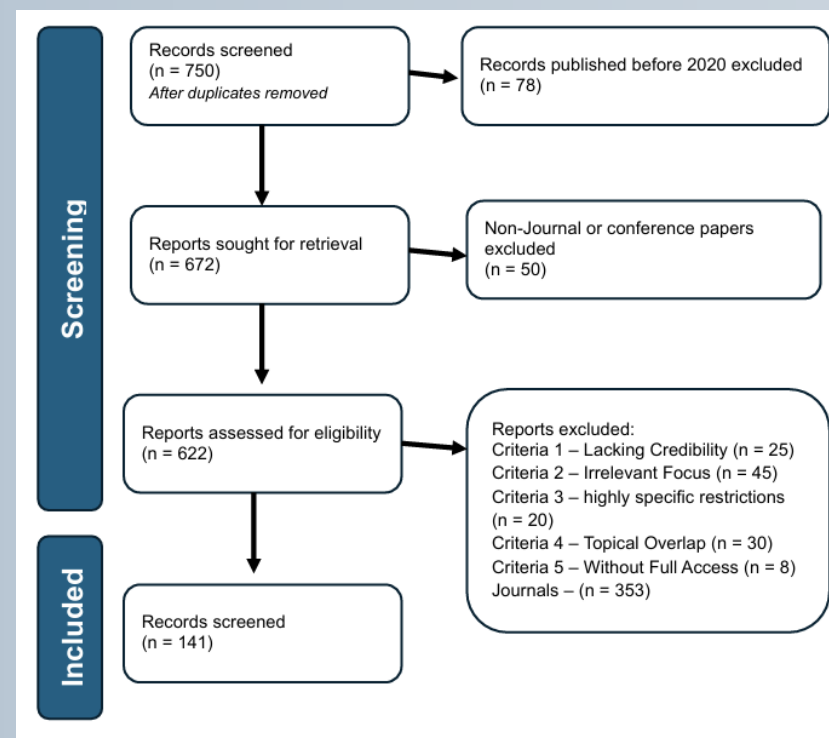


Figure 2. PRISMA Framework of Literature Review

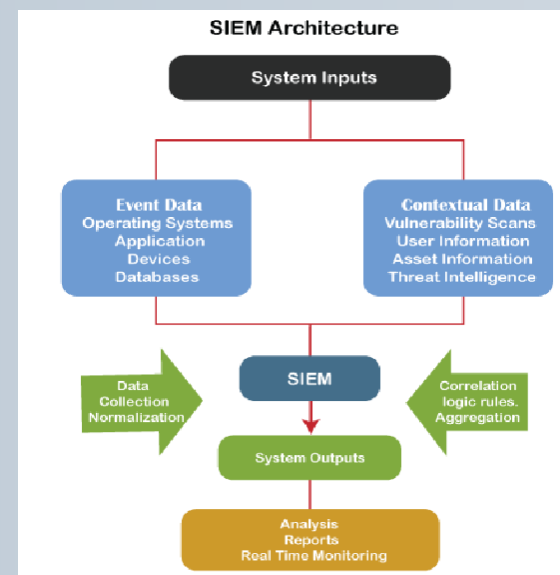


Figure 1. Diagram of SIEM Architecture [1]

5. Evaluation

Tested the automation flow exclusively in the DHCW Azure environment using scheduled simulated alerts. Over 500 alerts processed in 3 days, including overnight runs, to assess accuracy, reliability, and repeatability.

Key metrics:

- Accuracy – GeoIP enrichment returned correct Country, City, Latitude, and Longitude.
- Impact – Reduced manual triage by providing context directly in the incident comment.
- Reliability – Workflow triggered and completed successfully after early fixes.

Results confirmed the workflow met objectives and provided a solid base for future automation enhancements. Early challenges included duplicate IP entity and case sensitivity in KQL; both resolved for stable operation. Due to Azure and DHCW restrictions 8-hour maximum period was allowed for working before needed new approval. Due to current job role being outside the scope of this project additional learning and research was required to complete this project.

6. Conclusion

This was a development project set out to design and implement an automation process in Microsoft Sentinel. This would enrich alert data and reduce manual investigation time. The main aim was to improved efficiency through the integration of Logic Apps and GeoIP enrichment. Implementation was achieved by creating a Playbook, configuring action to manage alert data.

This demonstrated that alerts to the Security Operations Centre (SOC) can be enriched and triaged, aiding the detection and improving the timely resolution of alerts. Adjustments made and insights gained provided a support for incorporating further automation within the wider security workflow.

Although this project used a test environment, lessons learned from this project can be applied to future versions of Microsoft Sentinel using live data.

References

- [1] M. Jhaveri and V. Parmar, 'CLOUD Security Information and Event Management CLOUD Security Information & Event Management'. [Online]. Available: <https://www.researchgate.net/publication/369302413>
- [2] 'Digital and data strategy for health and social care in Wales'. [Online]. Available: <https://www.gov.wales/digital-and-data-strategy-health-and-social-care-wales-html>
- [3] Welsh Assembly Government, 'Cyber action plan for Wales', May 2023. [Online]. Available: <https://www.gov.wales/cyber-action-plan-wales-html>