**Large Language Models (LLMs) and their application in Cybersecurity**  
***Project Team***

|  |  |
| --- | --- |
| Full Name | Student ID |
| Shuhan Yan | s4913324 |
| Xiaozhe Liu | s4901089 |
| Boya Feng | s4951799 |
| Yuexuan Yang | s4844302 |

### ***Project Goals & Motivation***

The integration of SIEM (Security Information and Event Management) with Machine Learning (ML) aims to enhance threat detection, reduce false positives, accelerate response times, and automate security analysis. Traditional SIEM relies on rule-based methods, making it difficult to detect emerging attacks, whereas ML can learn normal behavior patterns, identify anomalies, and improve detection accuracy. With increasingly complex cyber threats, SOC (Security Operations Centers) face overwhelming alerts—ML helps analyze data intelligently, reducing manual workload and prioritizing threats more effectively. Additionally, as cloud computing and remote work expand the attack surface, ML enables adaptive threat detection. Overall, combining SIEM with ML makes cybersecurity more intelligent and real-time, strengthening enterprise security posture.

### ***Project Methodology***

1.Define the research theme and focus on a specific problem, such as improving the security detection capabilities of SIEM combined with machine learning.

2.Search for relevant literature in academic databases and select high-quality, relevant papers based on the research objectives.

3.Read the selected papers in detail, analyzing their methods, contributions, and limitations, and understanding the current progress in the field.

4.Categorize the papers by theme, summarize key findings, and identify research gaps and challenges.

5.Write a research summary report, outlining the key points from the literature review to provide a foundation for further research.

### ***Related Work***

Google AI: plays a crucial role in the field of machine learning by providing open-source tools, frameworks (such as TensorFlow), advanced research outcomes, and powerful computing platforms[1].

Splunk: discusses how SIEM integrates log management, event correlation, and automated responses to enhance security visibility, threat detection, and compliance. The article also highlights the value of advanced analytics and machine learning in improving risk management and operational efficiency[2].

## References

[1] G. AI. <https://ai.google/> (accessed April 1, 2025).

[2] Splunk. <https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html> (accessed April 1, 2025).