20230705 討論事項

1. Remove Sigma from system architecture. Sigma should be a baseline and move it to experiment section in my thesis.
2. Remove the concept of provenance graph from my thesis. Focus on detecting technique on one single event.
3. New system architecture：
    - Module1. Synthesize Audit Log
        - 如何模擬出含 attack 和 benign 的 log
    - Module2. Embedding Function
        - TransX, Rescal…
    - Module3. Detection Model
        - GNN, LSTM…

System Architecture

Module1.
Synthesize
Audit Log

Windows
Audit Logs

Module2.
Synthesize
Audit Log