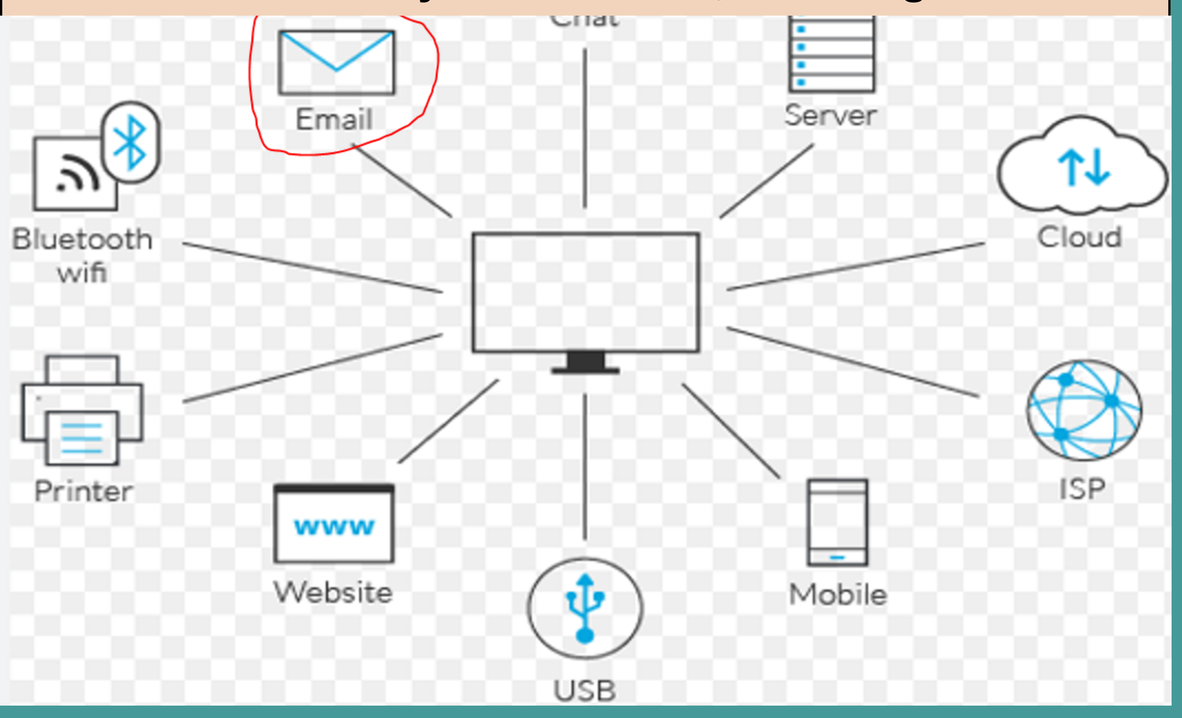
A comparative study of DLP strategies in email systems and their impact on SOC efficiency

Author: Edet Bassey | C00292045@setu.ie

Supervisor: Michael Gleeson

1. Introduction

- DLP in email systems safeguard sensitive information transmitted through email channels from unauthorized access or disclosure.
- Achieved through DLP technologies and strategies such as rule-base DLP policy, data classification, encryption, data access control, AI/ML, etc.
- DLP strategy in email system have impact on SOC efficiency
- The research goal is to identify best practices and recommend improvement to the existing DLP methods to optimize SOC efficiency based on research literature review and primary data collected through survey and interview.
- This research is significant for organization relying heavily on email communication by providing insights to enhance DLP strategies and optimize SOC operation. diagram below showing various data flow monitored by DLP solution, including email.



2. Research Questions

- RQ1: What are the characteristics, limitation and effectiveness of different DLP strategies in the email system
- RQ2: What are the impacts and challenges of different DLP strategies on key indicators of SOC efficiency
- RQ3: What recommendations can be derived from the DLP strategies evaluation to enhance organization email security and SOC efficiency

3. Literature Review

- Analysis of existing DLP strategies adopted in preventing and detecting data loss in email systems with traditional DLP strategies such as keyword filtering, content inspection, context analysis, attachment inspection, encryption, rule-based DLP policy were review, including their drawback on SOC efficiency such as excessive false positive alerts generation.
- Explored advance DLP strategies such as ML/AI, UEBA, SOAR, SIEM, and evaluate how these strategies impact SOC efficiency.
- Researchers suggest that traditional DLP strategies likely result in a lower SOC efficiency due to high volume of generated false positive alerts while Advance DLP strategies improve SOC efficiency due to lower false positive alerts generation from advance DLP

4. Research Methodology

- Mixed approach adopted which involve quantitative and qualitative approaches.
- Quantitative method - literature review of different DLP strategies in email systems to identify DLP features for evaluation and how they affect SOC efficiency.
- Qualitative method - Survey and interviews with Information Technology professionals that include SOC Analysts.
- Data analysis will involve correlations between DLP strategies from Literature review and professional experience obtain via survey and interview regarding DLP strategies impact on SOC team workload

5. Early indications/next steps

- Adoption of hybrid DLP strategies - combination of the traditional DLP strategies (rules based policy) and modern DLP strategies (ML/AI) for effective detection and prevention of data loss in email system and improving SOC efficiency.
- Integration of Explainable AI (XAI) with Email DLP solution
- The next steps is to analyze the primary data (survey and interview data) using thematic analysis to find the tthemes and then correlate with secondary data from the literature review.

6. References

- Jaakko Mansikka, (2023). DATA LOSS PREVENTION For Securing Enterprise Data Integrity.
- Mohammed Anwarul Islam, (2023). Application of artificial intelligence and machine learning in security operations center
- Adam Smejkal (2020). Tool for automatic enforcement of DLP policies in cloud applications.
- Singh, Kunal, (2020). Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab
- Mohamed Falah Faiz, Junaid Arshad, Mamoun Alazab, Andrii Shalaginov (2020). Predicting Likelihood of Legitimate Data Loss in Email DLP.