ABSTRACT

Development of a Wazuh SIEM for Preventing Access to Malicious URLs Using the Large Language Model based on BERT

Coenraad Samuel Marco Hursepuny.[1], Hendi Hermawan, S.T., M.T.I.[2]

[1] Student of Informatics Study Program, Pembangunan Jaya University

[2] Lecturer of Informatics Study Program, Pembangunan Jaya University

The threat posed by access to malicious URL*s remains a significant issue in modern network security, as such* URL*s are frequently exploited in phishing, malware distribution, and data theft attacks. This study aims to develop a Security Information and Event Management (*SIEM*) system capable of automatically detecting and preventing access to malicious* URL*s. The system is built using Wazuh as the* SIEM *platform and leverages a BERT-based Large Language Model (LLM) for* URL *classification. The methodology involves training the LLM on a labeled* URL *dataset, integrating the model into Wazuh via a Flask API, and implementing an Active Response mechanism to block harmful access in real time. Experimental results demonstrate that the system can detect and prevent malicious* URL *access with accuracy 98%, precision 97%, recall 98% and F1-score 98%. In conclusion, integrating LLM into Wazuh enhances the* SIEM*'s ability to respond to threats automatically and efficiently, able to show the alert directly on the SIEM and offering a practical contribution to network cybersecurity.*

Keywords: *Large Language Model*, BERT, *Malicious* URL, SIEM, Wazuh