ABSTRAK

Pengembangan SIEM Wazuh untuk mencegah akses URL Berbahaya dengan Large Language Model berbasis BERT

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

[1)] Mahasiswa Program Studi Informatika, Universitas Pembangunan Jaya

[2)] Dosen Program Studi Informatika, Universitas Pembangunan Jaya

Ancaman akses terhadap URL berbahaya (*malicious* URL) menjadi salah satu masalah signifikan dalam keamanan jaringan modern, karena sering dimanfaatkan dalam serangan *phishing*, *malware*, dan pencurian data. Penelitian ini bertujuan untuk mengembangkan sistem Security Information and Event Management (SIEM) yang mampu mendeteksi dan mencegah akses ke URL berbahaya secara otomatis. Sistem dibangun menggunakan Wazuh sebagai platform SIEM dan memanfaatkan Large Language Model (LLM) berbasis BERT untuk klasifikasi URL. Metodologi yang digunakan mencakup pelatihan model LLM dengan dataset URL, integrasi model ke dalam sistem Wazuh melalui API Flask, serta penerapan Active Response untuk memblokir akses berbahaya secara real-time. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi dan mencegah akses ke URL berbahaya dengan hasil nilai akurasi 98%, *precision* 97%, *recall* 98% dan *F1-score* 98%. Kesimpulannya, hasil dan integrasi LLM ke dalam Wazuh dapat meningkatkan kapabilitas SIEM dalam merespons ancaman secara otomatis, efisien, dapat ditunjukkan pada sistem SIEM dengan baik dan jelas, serta memberikan kontribusi nyata dalam meningkatkan keamanan siber jaringan.

Kata Kunci: *Large Language Model*, BERT, URL berbahaya, SIEM, Wazuh.