ABSTRAK

Dalam era digital ini, sistem informasi telah menjadi tulang punggung bagi banyak organisasi dan perusahaan. Sistem informasi digunakan untuk mengelola data, memfasilitasi komunikasi internal dan eksternal, menjalankan proses bisnis, dan menyediakan layanan kepada pengguna. Namun, penggunaan sistem informasi tidak terlepas dari ancaman serangan siber yang merugikan. Data statistik dari Badan Siber dan Sandi Negara (BSSN) mencatat telah terjadi 370,02 juta serangan siber di Indonesia pada tahun 2022. Angka ini menunjukkan peningkatan sebesar 38,72% dibandingkan dengan tahun 2021 yang mencatat 266,74 juta serangan siber. Ketika suatu organisasi, perusahaan, atau badan pemerintahan terkena serangan siber, hal ini dapat menyebabkan berbagai masalah seperti gangguan operasional, kerusakan reputasi, hilangnya data pelanggan dan rahasia, kehilangan bisnis, kerugian material, dan bocornya informasi perusahaan.

Berdasarkan data dari Otoritas Jasa Keuangan (OJK) yang dilaporkan di website Kompas, selama periode Semester I-2020 hingga Semester I-2021, serangan siber mengakibatkan kerugian pada sektor perbankan sebesar Rp 246,5 miliar. Secara global, Dana Moneter Internasional (IMF) memperkirakan kerugian akibat serangan siber mencapai Rp 1.420 triliun per tahun. Melihat dampak yang signifikan dari serangan siber, penting bagi organisasi, perusahaan, dan badan pemerintahan untuk memiliki sistem yang dapat memantau, menganalisis kerentanan, dan mencegah serangan siber. Sistem pemantauan, analisis kerentanan, dan pencegahan terhadap serangan siber ini dapat berupa Intrusion Detection System (IDS) yang mampu mendeteksi dan mencegah serangan siber.

Wazuh merupakan platform open source yang berperan sebagai Intrusion Detection System (IDS) atau sistem deteksi ancaman, pemantauan keamanan, dan respons insiden. Implementasi Wazuh dapat menjadi tembok pertahanan dalam suatu organisasi, perusahaan, atau badan pemerintahan dalam mengatasi serangan siber. Wazuh memiliki berbagai fungsi penting, termasuk pencegahan ancaman, pemantauan integritas, respons terhadap insiden, kepatuhan terhadap standar keamanan, manajemen log peristiwa, dan deteksi celah keamanan. Dengan mengimplementasikan Wazuh, organisasi dapat meminimalisir risiko dan dampak dari serangan siber, serta meningkatkan keamanan dan ketahanan sistem informasi mereka.