ABSTRAK

In this digital era, information systems have become the backbone of many organizations and companies. Information systems are used to manage data, facilitate internal and external communication, execute business processes, and provide services to users. However, the use of information systems is not free from the threat of damaging cyberattacks. Statistical data from the National Cyber and Crypto Agency (BSSN) recorded 370.02 million cyberattacks in Indonesia in 2022. This figure represents an increase of 38.72% compared to 2021, which saw 266.74 million cyberattacks. When an organization, company, or government body is hit by a cyberattack, it can lead to various issues such as operational disruptions, reputational damage, loss of customer and confidential data, business loss, material damage, and leakage of company information.

According to data from the Financial Services Authority (OJK) reported on the Kompas website, during the period from the first half of 2020 to the first half of 2021, cyberattacks resulted in losses amounting to IDR 246.5 billion in the banking sector. Globally, the International Monetary Fund (IMF) estimates the annual loss from cyberattacks to reach IDR 1,420 trillion. Given the significant impact of cyberattacks, it is crucial for organizations, companies, and government bodies to have systems in place that can monitor, analyze vulnerabilities, and prevent cyberattacks. Such systems can include an Intrusion Detection System (IDS) capable of detecting and preventing cyberattacks.

Wazuh is an open-source platform that functions as an Intrusion Detection System (IDS) or a threat detection, security monitoring, and incident response system. Implementing Wazuh can serve as a defensive wall for an organization, company, or government body in combating cyberattacks. Wazuh offers various essential functions, including threat prevention, integrity monitoring, incident response, compliance with security standards, event log management, and security gap detection. By implementing Wazuh, organizations can minimize the risks and impacts of cyberattacks, as well as enhance the security and resilience of their information systems.