IMPLEMENTATION OF MOBILE SIEM FOR REAL-TIME NETWORK THREAT NOTIFICATION AND RESPONSE

Student Name	:	Ilman Sholihin
Student ID Number	:	6404221146
Supervisor	:	Nurmi Hidayasari, S.T., M.Kom
		Mansur, S.Kom., M.Kom

ABSTRACT

Network security is a vital aspect of maintaining the stability of information systems in the digital era. Security Information and Event Management (SIEM) systems such as Wazuh are widely used to detect threats; however, these systems have mobility limitations because Dashboards are only web-based and notifications depend on third-party platforms, making it difficult for administrators to respond quickly to security incidents. This study aims to develop a Wazuh-based mobile SIEM application capable of providing real-time network security notifications along with initial response recommendations for detected threats. The research uses an experimental approach involving integration with the Wazuh API, development of Python-Flask–based middleware, implementation of Firebase Cloud Messaging (FCM), and development of a Flutter mobile application. Testing was conducted using three attack scenarios SQL Injection, Cross-Site Scripting (XSS), and Web Directory Scanning with five trials each. The results show that the system successfully detected attacks with an average Detection Latency of 1.69 seconds, notification latency of 0.82 seconds, and End-to-End Latency of 2.51 seconds, while effectively delivering real-time security notifications to mobile devices and providing initial response recommendations that can serve as mitigation guidance for network administrators.

Kata kunci: *SIEM, Wazuh, Mobile Security, Real-time Notification, Flutter, Network Security*