ABSTRACT

This study aims to explore and analyze the effectiveness of implementing open-source Security Information and Event Management (SIEM) using Elastic Security in detecting increasingly complex cyber threats. The primary focus of the research is on integrating Threat Intelligence and Threat Behavior to enhance threat detection capabilities in SIEM. Elastic Security is utilized in this study to manage and analyze log data generated by systems and applications connected to the organization's network.

The research was conducted through a series of experiments involving various types of cyber attacks, including port scanning, brute force, and Distributed Denial of Service (DDoS). The experiments were conducted in a virtual environment configured using VMware to simulate the target server (CentOS) and the attacker machine (Kali Linux). In each experiment, the method involved analyzing the logs generated by Elastic Security to evaluate the effectiveness of threat detection and response.

The results of the study show that Elastic Security is capable of detecting most types of attacks with high accuracy, particularly port scanning and brute force attacks, with varying response times. The Nmap - Zenmap GUI (Intense Scan, All TCP) attack was detected the fastest within 15 seconds, while the Nmap - Zenmap GUI (Intense Scan plus UDP) attack was detected the slowest in 9 minutes and 41 seconds. However, there are weaknesses in detecting DDoS attacks and brute force attacks conducted with the Medusa tool, which were not detected at all, indicating the need for improvements in detection configurations and rules. Additionally, the risk metrics indicate that the Nping Process Activity used to detect DDoS attacks and Potential Internal Linux SSH Brute Force used to detect Brute Force Attacks have the highest risk scores of 47 with a medium severity level, while the potential detection of port scanning has a risk score of 21 with a low severity level.

Elastic Security is effective in detecting port scanning and brute force attacks, but it shows weaknesses in detecting DDoS attacks and brute force attacks using Medusa. The highest risk scores were found in Nping Process Activity and

Potential Internal Linux SSH Brute Force. To enhance effectiveness, improvements in configuration, detection rules, and better integration with Threat Intelligence and Behavior Profiling are necessary.

Keywords — **Elastic Security, SIEM, Threat Intelligence, Behavior Profiling, Threat Detection.**