ABSTRACT

The rapid advancement of information technology has increased the need for cybersecurity systems capable of effectively detecting and analyzing threats. One commonly adopted approach involves integrating Host-based Intrusion Detection Systems (HIDS) with threat analysis frameworks such as the MITRE ATT&CK. However, during the analysis of logs and incidents using tools like Wazuh and Elasticsearch, it was discovered that the generated alerts or rules were not yet fully mapped to the MITRE ATT&CK framework. This lack of automatic mapping made it difficult to identify the corresponding attack tactics and techniques, thereby limiting the effectiveness of incident analysis. To address this issue, this research focuses on developing a solution by creating and customizing specific detection rules that automatically associate each alert or incident with the appropriate tactics and techniques in MITRE ATT&CK. A testing environment was built by integrating Wazuh as the HIDS and Elasticsearch as the log storage and analysis engine. This approach enables real-time and contextual classification of detected incidents, significantly improving the speed, accuracy, and depth of incident analysis. The results of this study show that automated mapping can enhance the effectiveness of threat detection and incident response processes.

Keywords: *Wazuh, MITRE ATT&CK, Elasticsearch, Cybersecurity, Rule Mapping, Threat Detection*.