ABSTRACT

Intrusion Detection System (IDS) is one of the important mechanisms in maintaining network security. IDS is divided into two based on its detection method, namely signature and anomaly. The signature method has weaknesses in detecting unknown attacks, while the anomaly method can detect unknown attacks but tends to produce high false positives. This study proposes a hybrid model that combines Suricata as the signature component and Isolation Forest as the anomaly component. The hybrid model enables the detection of attacks with unknown patterns that cannot be handled by the signature method alone. To limit the false positives generated by the anomaly component, this study proposes an additional mechanism in the form of gating using a watchlist at the final decision level of the system. Testing in this study was conducted on the CIC-IDS2017 dataset with two main scenarios, namely known attacks and unknown attacks. Without gating, the hybrid model produced a fairly high false positive rate. With the watchlist mechanism at the decision level, the hybrid model successfully limited the FPR from 34.74% to 0.063% in the known attack scenario and limited the FPR from 33.82% to 0.486% in the unknown attack scenario. In addition, the model also had better attack detection performance compared to the standalone model. In the known attack scenario, attack detection performance increased by 1.58% compared to Suricata. In the unknown attack scenario, attacks that failed to be detected by Suricata were successfully detected by the hybrid model with a value of 80%. This capability comes with the consequence of a significant increase in computing resources.

Keywords: *anomaly, Intrusion Detection System, hybrid, signature, unknown attack*