***Abstract* — The application of an Intrusion Detection System (IDS) using machine learning techniques that are integrated with Security Information & Event Management (SIEM) on a large-scale network will increase the security of the network because the machine learning-based IDS system can detect anomalies in every packet that assessed from the behavior of the packet so that it can reduce the occurrence of an attack on the network, compared to using rule-based and signature-based IDS which cannot adapt to every packet generated by the IDS. In this paper, the proposed system performs well in the DoS test with 344.1/sec packet to test whether the system can overcome the DoS. The result of 4 components consists of Elasticsearch, Logstash, Kibana and Zeek, which are monitored to see the system usage. Elasticsearch is the most component that uses system CPU and RAM at 78% of CPU usage and 2300 Mb of RAM usage, and the least consumed system usage is Zeek with 3.5% CPU usage and 225 Mb RAM usage.**

Keywords — (IDS, SIEM, Machine Learning)