ABSTRAK

ANALISA PERBANDINGAN KINERJA MONITORING *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) MENGGUNAKAN *SPLUNK* DAN *ELASTIC STACK* DARI SERANGAN SIBER

Oleh :

M. HENDRO JUNAWARKO

18312215

Permasalahan tentang adanya serangan siber terhadap suatu perusahaan atau organisasi sering terjadi, hal tersebut dikarenakan semakin berkembangnya teknologi maka semakin berkembang juga ancaman dan resiko yang dapat merusak sistem dan membocorkan data penting dari suatu perusahaan. Keamanan jaringan menjadi hal yang sangat penting untuk diamati dan dilindungi. Salah satu cara untuk melindungi jaringan adalah dengan menggunakan *Security Information and Event Management* (SIEM). *Splunk* dan *Elastic Stack* adalah beberapa contoh dari SIEM sebagai solusi teknologi yang digunakan untuk membantu dalam mengumpulkan, menganalisis dan melaporkan informasi keamanan dari berbagai sumber.

Oleh sebab itu, penulis melakukan perbandingan kinerja menggunakan *Splunk* dan *Elastic Stack* sebagai *Security Information and Event Management* (SIEM) dari serangan siber. Serangan yang akan dilakukan dalam penelitian ini yaitu *Port Scannning*, *Bruteforce Attack* dan *DoS Attack*. Hasil dari analisa perbandingan kinerja masing-masing SIEM tersebut menunjukkan *Splunk* lebih unggul di nilai rata-rata penggunaan *resource* CPU sebesar 20,6% dan RAM sebesar 45%, kecepatan *ingest log* sebesar 11 detik dan waktu notifikasi *alert* sebesar 12,1 detik. Sedangkan Elastic Stack lebih unggul dari deteksi alert serangan dengan nilai rata-rata sebesar 48 *Alert*.

Kesimpulan dari penelitian yang telah dilakukan berdasarkan semua pengujian tersebut menunjukkan bahwa setiap SIEM berhasil mendeteksi *alert* serangan dan mengirimkan notifikasi email, dengan hasil *Splunk* lebih baik daripada *Elastic Stack* dalam penggunaan *resource* CPU dan RAM, juga pada kecepatan *ingest log* dan waktu notifikasi *alert email*. Sedangkan untuk deteksi *alert* serangan, *Elastic Stack* lebih unggul dari pada *Splunk*

Kata Kunci: *Security Information and Event Management*, *SIEM, Keamanan Jaringan, Splunk, Elastic Stack*