INTISARI

Analisis Performa *High Availability Security Operation Center* Menggunakan Docker Swarm dengan Teknik *Failover* di PT. Emporia Digital Raya

Seiring perkembangan teknologi, keamanan *(security)* dan ketersediaan *(availability)* sistem informasi juga dituntut untuk semakin tinggi. Sebagai perusahaan yang bergerak di bidang teknologi, PT. Emporia Digital Raya menggunakan wazuh sebagai sistem *Security Information and Event Management* (SIEM) yang berfungsi untuk melakukan monitoring pada setiap server. Akan tetapi, akan menjadi masalah ketika aplikasi tidak berjalan semestinya karena terjadi permasalahan pada *container* sehingga diperlukan *high availability* sistem. Docker memiliki fitur untuk melakukan manajemen aplikasi dengan menggunakan docker swarm. Docker swarm memungkinkan pengguna untuk mengelola beberapa *container* yang digunakan di beberapa virtual mesin. Implementasi *high availability* dengan teknik *failover* adalah ketika layanan mengalami kegagalan, maka *container* di server lain akan mengambil alih dan *service* yang mengalami masalah akan melakukan perbaikan secara otomatis. Penelitian ini menunjukkan bahwa sistem *high availability security operation center* menggunakan docker swarm dengan teknik *failover* memberikan performa kinerja yang baik dengan *downtime* sebesar 211,2 detik sehingga sistem dapat menjadi solusi permasalahan kegagalan layanan pada *security operation center*. Performa sistem secara fungsional mengalami penurunan rata-rata waktu deteksi serangan sebesar 12,9% pada penyerangan *brute-force* ssh dan 5,98% pada *port scanning,* serta penggunaan *resource* CPU dan *memory* yang lebih kecil dibandingkan dengan *security operation center*.

Kata kunci: Docker Swarm, *Failover*, *High Availability*, Wazuh

ABSTRACT

Performance Analysis of High Availability Security Operation Center Using Docker Swarm with Failover Technique at PT. Emporia Digital Raya

Along with the development of technology, the security and availability of information systems are also required to be higher. As a company engaged in technology, PT. Emporia Digital Raya uses wazuh as a Security Information and Event Management (SIEM) system that functions to monitor each server. However, it will be a problem when the application does not run properly due to problems with the container so that a high availability system is needed. Docker has a feature to perform application management using the docker swarm. Docker swarm allows users to manage multiple containers deployed across multiple virtual machines. The implementation of high availability with the failover technique is when a service fails, the container on another server will take over and the service that has a problem will make repairs automatically. This study shows that the high availability security operation center system using a docker swarm with failover technique provides good performance with a downtime of 211.2 seconds so that the system can be a solution to service failure problems at the security operation center. Functional system performance decreased the average attack detection time by 12.9% on brute-force ssh attacks and 5.98% on port scanning, as well as less CPU and memory resource usage compared to the security operation center..

Keyword : Docker Swarm, Failover, High Availability, Wazuh