UNIVERSITAS
GADJAH MADA
RANCANGAN DAN IMPLEMENTASI WAZUH OPEN SOURCE SECURITY PLATFORM MENGGUNAKAN METODE DISTRIBUTED DEPLOYMENT PADA DOCKER CONTAINER UNTUK MONITORING VIRTUAL PRIVATE SERVER DI PT. EMPORIA DIGITAL RAYA
ARDITA, Hidayat Nur Isnianto, S.T., M.Eng
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

RANCANGAN DAN IMPLEMENTASI *WAZUH OPEN SOURCE SECURITY PLATFORM* MENGGUNAKAN METODE *DISTRIBUTED DEPLOYMENT* PADA *DOCKER CONTAINER* UNTUK *MONITORING VIRTUAL PRIVATE SERVER* DI PT. EMPORIA DIGITAL RAYA

Abstract — PT. Emporia Digital bergerak dalam bidang finansial teknologi memiliki *virtual private server* yang belum menerapkan *security operation center*. Layanan finansial teknologi rentan terhadap kejahatan siber. Oleh karena itu diperlukan *security operation center* untuk mengamati keamanan server. Penelitian ini menggunakan wazuh dan *elasticstack* sebagai layanan *security operation center* serta docker container sebagai server *security operation center.* Metode *distributed deployment* digunakan untuk memecah sistem menjadi beberapa bagian yang saling terhubung. Penambahan nginx digunakan sebagai *load balancer* dan *reverse proxy*. Jika terjadi serangan, *security operation center* akan mengirimkan notifikasi dalam bentuk teks pada mattermost.

Hasil dari penelitian ini adalah layanan *security operation center* yang digunakan perusahaan dalam melakukan pemantauan keamanan server. Layanan tersebut menjadi data untuk laporan bulanan perusahaan terkait aktivitas keamanan server. Penggunaan mattermost bertujuan untuk menerima notifikasi serangan dari layanan *security operation center* sehingga *security operation center analyst* tidak perlu melakukan pengecekan server secara berkala.

Kata kunci : virtual private server, wazuh, elastic stack, docker container.

UNIVERSITAS
GADJAH MADA
RANCANGAN DAN IMPLEMENTASI WAZUH OPEN SOURCE SECURITY PLATFORM MENGGUNAKAN METODE DISTRIBUTED DEPLOYMENT PADA DOCKER CONTAINER UNTUK MONITORING VIRTUAL PRIVATE SERVER DI PT. EMPORIA DIGITAL RAYA
ARDITA, Hidayat Nur Isnianto, S.T., M.Eng
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

PT. Emporia Digital is engaged in financial technology has a virtual private server that has not implemented security operation center. Technology financial services are vulnerable to cybercrime. Therefore, it is necessary for security operation center to observe server security. This research uses wazuh and elasticstack as security operation center services as well as docker container as security operation center servers. The distributed deployment method is used to break the system into multiple interconnected parts. The addition of nginx is used for load balancers and reverse proxies. In the event of an attack, the security operation center will send a notification in the form of text on mattermost.

The result of this study is a security operation center service used by companies in monitoring server security. The service becomes data for the company's monthly reports on server security activities. The use of mattermost aims to receive attack notifications from the security operation center service so that security operation center analysts do not need to check the server periodically.

Keywords: virtual private server, wazuh, elastic stack, docker container