INTISARI

USULAN PROYEK AKHIR
PERANCANGAN *OPEN-SOURCE SECURITY ORCHESTRATION AUTOMATION AND RESPONSE* MENGGUNAKAN *WAZUH OPEN-SOURCE SECURITY PLATFORM* DAN *THEHIVE*

Abstract - Salah satu upaya untuk melindungi *virtual private server* dari serangan siber adalah dengan penerapan *security operation center* (SOC). *Security operation center* (SOC) bertanggung jawab untuk memantau, menganalisis, dan mengurangi ancaman yang masuk. Di dalam *security operation center* terdapat pendekatan *security information and event management* yang digunakan oleh analis *security operation center* sebagai titik pusat di mana semua peringatan keamanan dari berbagai teknologi keamanan disimpan, dikumpulkan dan ditampilkan termasuk *firewall*, IPS/IDS, dan *log antivirus*.

Security operation center (SOC) dalam suatu organisasi memiliki perangkat dan pendekatan yang biasa digunakan yaitu *security information and event management* (SIEM). Akan tetapi perkembangan jenis dan banyaknya serangan yang berkembang mengakibatkan munculnya serangan dan insiden baru. Hal tersebut membutuhkan fungsionalitas lebih pada *tool* yang sudah banyak digunakan sekarang ini. Pendekatan *security orchestration automation and response* (SOAR) dapat digunakan pada sebuah organisasi guna meningkatkan informasi analisis log. Implementasi wazuh, shuffle dan TheHive mampu membentuk *security orchestration automation and response* (SOAR).

Kata kunci*: SOC, SIEM, SOAR, Wazuh, TheHive*

ABSTRACT

One of the efforts to protect virtual private servers from cyber attacks is by implementing a security operation center (SOC). The security operation center (SOC) is responsible for monitoring, analyzing, and mitigating incoming threats. Within the security operation center there is a security information and event management approach used by security operation center analysts as the central point where all security alerts from various security technologies are stored, collected and displayed including firewall, IPS/IDS, and antivirus logs.

Security operation center (SOC) in an organization has tools and approaches commonly used, namely security information and event management (SIEM). However, the development of the type and number of attacks that developed resulted in the emergence of new attacks and incidents. This requires more functionality in the tools that are widely used today. The security orchestration automation and response (SOAR) approach can be used in an organization to improve log analysis information. The implementation of wazuh, shuffle and TheHive is able to form a security orchestration automation and response (SOAR).

Keywords: SOC, SIEM, SOAR, Wazuh, TheHive