Universitas Indonesia Library >> UI - Skripsi Membership

Analisis implementasi Security Information and Event Management (SIEM) dengan berbasis wazuh pada sistem operasi Windows dan Linux = Analysis of Security Information and Event Management (SIEM) implementation based on wazuh on Windows and Linux operating systems

Dimas Radhitya, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20523053&lokasi=lokal

---

Abstrak

Wazuh merupakan sistem Security Information Event Management (SIEM) dan aplikasi open-source host-based intrusion detection sistem (HIDS) yang dapat melakukan memantau infrastruktur, mendeteksi ancaman, upaya penyusupan, anomali sistem, penilaian konfigurasi, dan tindakan pengguna yang tidak sah. Wazuh juga menyediakan kerangka kerja untuk respons insiden dan kepatuhan terhadap peraturan (Regulatory Compliance). Penelitian ini akan mengembangkan Wazuh dengan mengintegrasikan tiga Application Programming Interface (API) untuk meningkatkan kinerja Wazuh sebagai sistem SIEM. Penelitian ini akan membandingkan Wazuh dengan Solarwinds SEM untuk membandingkan kinerja dari kedua sistem SIEM dengan melakukan lima skenario penyerangan. Skenario tersebut dilakukan untuk menguji kinerja deteksi serangan dari kedua sistem SIEM. Sebelum scenario dilakukan penulis mengintegrasikan tiga API yaitu VirusTotal, Yara dan Suricata untuk memaksimalkan kinerja sistem SIEM Wazuh. Sistem SIEM Wazuh mempunyai akurasi sebesar 100% dalam mendeteksi seluruh serangan yang dilakukan sementara sistem SIEM Solarwinds SEM hanya mempunyai akurasi sebesar 40% dalam mendeteksi kelima skenario.

.....Wazuh is a Security Information Event Management (SIEM) and open-source host-based intrusion detection system (HIDS) application that can monitor infrastructure, detect threats, intrusion attempts, system anomalies, configuration assessments, and unauthorized user actions. Wazuh also provides a framework for incident response and regulatory compliance. This research will develop Wazuh by integrating three Application Programming Interfaces (API) to improve Wazuh's performance as a SIEM system. This study will compare Wazuh with Solarwinds SEM to compare the performance of the two SIEM systems by performing five attack scenarios. The scenario was carried out to test the attack detection performance of the two SIEM systems. Before the scene was carried out, the author integrated three APIs, namely VirusTotal, Yara, and Suricata to maximize the performance of the Wazuh SIEM system. The Wazuh SIEM system has 100% accuracy in detecting all attacks carried out while the Solarwinds SEM SIEM system only has 40% accuracy in detecting all five scenarios.