ABSTRAK

Salah satu teknologi yang berkembang pesat hingga saat ini adalah *Internet*. Pesatnya perkembangan *Internet* ini disebabkan oleh kebutuhan manusia yang semakin beragam juga. Berkembang pesatnya *Internet* tidak hanya menimbulkan efek positif, namun negatifnya juga. Salah satu efek negatif dari *Internet* yaitu serangan *Malware*. Dalam penelitian ini akan dilakukan analisis terhadap serangan *malware* menggunakan konsep SIEM (*Security Information and Event Management*) dengan tujuan untuk mengidentifikasi suatu serangan *malware*, menganalisa kemampuan SIEM dalam menangani serangan *malware*, dan tentu mencari solusi untuk menangani suatu serangan *malware* pada sistem. Penelitian ini akan dilakukan menggunakan sistem operasi Windows 10, Debian 11 dan disertai juga dengan *tools* seperti VirusTotal dan Wazuh. Wazuh di sini adalah sebagai implementasi dari konsep SIEM yang digunakan dalam penelitian ini. Dengan dilakukannya konfigurasi antara Wazuh dengan VirusTotal, maka hasil yang diharapkan adalah dapat dihasilkan otomasi berupa *alert* ke Wazuh dan *auto remove file* terhadap *file* yang terdeteksi sebagai *malware*.

Kata Kunci: SIEM, *Malware*, Wazuh.

ABSTRACT

One of the technologies that has developed rapidly until now is the Internet. The rapid development of the Internet is due to the increasingly diverse human needs as well. The rapid development of the Internet not only has a positive effect, but also a negative one. One of the negative effects of the Internet is malware attacks. In this study, analysis of malware attacks will be carried out using the concept of SIEM (Security Information and Event Management) with the aim of identifying a malware attack, analyzing the ability of SIEM to handle malware attacks, and of course finding solutions to deal with a malware attack on the system. This research will be conducted using the Windows 10 operating system, Debian 11 and also accompanied by tools such as VirusTotal and Wazuh. Wazuh is an application that is used as an implementation of the SIEM concept in this study. With the configuration between Wazuh and VirusTotal, the expected result is that an automation can be generated in the form of alerts to Wazuh and an auto remove file against the file that detected as malware.

Keyword: SIEM, Malware, Wazuh.