ABSTRACT

Cyber threats continue to increase as information technology advances, with malware as one of the main forms of threats that exploit security gaps. Security Information and Event Management (SIEM) such as Wazuh is an effective solution to detect and respond to cyber threats. However, malware detection performance by Wazuh Default is still limited by the API, with low accuracy (33%) and low recall (32%). This research aims to optimize malware detection through the integration of Wazuh with Cyber Threat Intelligence (CTI) using Malware Information Sharing Platform (MISP) and DFIR-IRIS. The results showed that the integration of MISP improved detection accuracy up to 62.3%, and threat detection precision reached 97.5%. However, the recall (62.4%) still showed that there were threats that were missed. The addition of DFIR-IRIS enables real-time incident response, improving mitigation efficiency. The combination of MISP and DFIR-IRIS significantly strengthens SIEM's detection and response capabilities, providing a more effective and comprehensive solution to cyber threats.

Keywords – *CTI, DFIR-IRIS, Malware Detection, MISP, SIEM WAZUH*

ABSTRAK

Ancaman siber terus meningkat seiring kemajuan teknologi informasi, dengan malware sebagai salah satu bentuk ancaman utama yang mengeksploitasi celah keamanan. *Security Information and Event Management (SIEM)* seperti *Wazuh* menjadi solusi efektif untuk mendeteksi dan merespons ancaman siber. Namun, performa deteksi malware oleh *Wazuh Default* masih terbatas oleh *API*, dengan akurasi rendah (33%) dan recall rendah (32%). Penelitian ini bertujuan mengoptimalkan deteksi malware melalui integrasi *Wazuh* dengan *Cyber Threat Intelligence (CTI)* menggunakan *Malware Information Sharing Platform (MISP)* dan *DFIR-IRIS*. Hasil penelitian menunjukkan bahwa integrasi *MISP* meningkatkan akurasi deteksi hingga 62,3%, serta presisi deteksi ancaman mencapai 97,5%. Meskipun demikian, *recall* (62,4%) masih menunjukkan adanya ancaman yang terlewat. Penambahan *DFIR-IRIS* memungkinkan respons insiden secara real-time, meningkatkan efisiensi mitigasi. Kombinasi *MISP* dan *DFIR-IRIS* memperkuat kemampuan deteksi dan respons *SIEM* secara signifikan, memberikan solusi yang lebih efektif dan menyeluruh dalam menghadapi ancaman siber.

Kata Kunci - *CTI,Deteksi Malware, DFIR-IRIS, MISP,SIEM WAZUH*