INTISARI

Ransomware LockBit 3.0 merupakan ancaman serius yang mampu mengganggu operasional sistem informasi serta menimbulkan kerugian signifikan. Penelitian ini membandingkan efektivitas integrasi YARA Rules dan VirusTotal pada sistem Wazuh dalam mendeteksi ransomware tersebut melalui metode eksperimen pada lingkungan virtual berbasis Ubuntu dan Windows, dengan tiga indikator evaluasi utama yaitu akurasi deteksi, waktu respons, dan penggunaan sumber daya sistem. Hasil pengujian menunjukkan bahwa integrasi YARA Rules mencapai akurasi deteksi 100% pada seluruh endpoint, memiliki waktu respons lebih cepat, dan konsumsi CPU serta memori lebih efisien dibandingkan VirusTotal. Sebaliknya, integrasi VirusTotal tidak berhasil mendeteksi sampel ransomware yang diuji karena ketergantungannya pada basis data hash yang telah dikenal sebelumnya, serta menunjukkan waktu respons lebih lambat dengan penggunaan sumber daya yang relatif lebih tinggi. Temuan ini menegaskan bahwa pemilihan metode integrasi pada Wazuh perlu disesuaikan dengan kebutuhan lingkungan operasional, di mana YARA Rules lebih unggul untuk deteksi varian baru, sedangkan VirusTotal lebih sesuai untuk verifikasi berbasis reputasi file.

Kata kunci: Wazuh, YARA Rules, VirusTotal, LockBit 3.0, ransomware

ABSTRACT

LockBit 3.0 ransomware poses a significant threat to information systems, potentially causing severe operational disruptions and substantial losses. This study compares the effectiveness of YARA Rules and VirusTotal integration within the Wazuh system for detecting this ransomware through an experimental approach in virtual environments running Ubuntu and Windows, evaluating three main performance indicators: detection accuracy, response time, and system resource usage. The results indicate that YARA Rules integration achieved 100% detection accuracy across all endpoints, demonstrated faster response times, and consumed CPU and memory resources more efficiently than VirusTotal. In contrast, VirusTotal integration failed to detect the tested ransomware samples due to its reliance on previously known hash databases, resulting in slower response times and relatively higher resource usage. These findings highlight that the choice of integration method should align with operational requirements, with YARA Rules being more suitable for detecting new ransomware variants, while VirusTotal serves better for file reputation-based verification.

Keyword: Wazuh, YARA Rules, VirusTotal, LockBit 3.0, ransomware