ABSTRACT

Cybersecurity is a crucial aspect in ensuring the continuity of business operations, especially in mitigating threats such as brute force attacks and malware. This study compares the effectiveness of two Security Information and Event Management (SIEM) systems, Wazuh and LogRhythm with their respective integrations, VirusTotal and CrowdStrike Falcon, in detecting and responding to cyber threats. The Pyramid of Pain methodology is applied to assess the difficulty attackers face based on the indicators used in threat detection. The findings indicate that LogRhythm with CrowdStrike Falcon excels in machine learning-based detection, allowing the identification of new threats even if they are not yet listed in malware databases. The results indicate that LogRhythm with CrowdStrike Falcon excels in machine learning-based threat detection, enabling the identification of new threats even if they are not yet listed in malware databases. Meanwhile, Wazuh, integrated with VirusTotal, offers hash-based and file reputation detection with greater transparency and no additional cost. The implementation of the Pyramid of Pain method in Wazuh enhances the detection of brute force attacks and malware, making it a strong competitor to LogRhythm. With its open-source nature allowing customization to user needs, Wazuh provides a more flexible and cost-effective option, while LogRhythm remains superior in pattern-based threat analysis. Therefore, the choice of SIEM should align with the organization's priorities, whether prioritizing flexibility and transparency or AI-based threat detection.

Keywords: *Cybersecurity, Wazuh, LogRhythm, Pyramid of Pain, SIEM, VirusTotal, CrowdStrike Falcon*

ABSTRAK

Keamanan siber menjadi aspek krusial dalam menjaga keberlangsungan operasional perusahaan, terutama dalam menghadapi ancaman seperti serangan *brute force* dan *malware*. Penelitian ini membandingkan efektivitas dua sistem keamanan informasi dan manajemen peristiwa (SIEM), yaitu *Wazuh* dan *LogRhythm* dengan integrasi masing-masing, yaitu *VirusTotal* dan *CrowdStrike Falcon*, dalam mendeteksi dan merespons ancaman siber. Implementasi metode *Pyramid of Pain* digunakan untuk mengukur tingkat kesulitan yang dihadapi penyerang berdasarkan indikator yang digunakan dalam deteksi. Hasil penelitian menunjukkan bahwa LogRhythm dengan *CrowdStrike Falcon* lebih unggul dalam deteksi berbasis *machine learning*, memungkinkan identifikasi ancaman baru meskipun belum terdaftar dalam database *malware*. Hasil penelitian menunjukkan bahwa *LogRhythm* dengan *CrowdStrike Falcon* unggul dalam deteksi berbasis *machine learning*, memungkinkan identifikasi ancaman baru meskipun belum terdaftar dalam database *malware*. Sementara itu, *Wazuh* dengan integrasi *VirusTotal* menawarkan deteksi berbasis hash dan reputasi file dengan transparansi lebih tinggi tanpa biaya tambahan. Penerapan metode *Pyramid of Pain* pada *Wazuh* meningkatkan efektivitas deteksi serangan *brute force* dan *malware*, menjadikannya pesaing kuat bagi *LogRhythm*. Dengan sifat *open-source* yang memungkinkan modifikasi sesuai kebutuhan, *Wazuh* menjadi pilihan yang lebih fleksibel dan ekonomis, sementara *LogRhythm* lebih unggul dalam analisis ancaman berbasis pola. Oleh karena itu, pemilihan SIEM harus disesuaikan dengan kebutuhan organisasi, apakah lebih mengutamakan fleksibilitas dan transparansi atau deteksi berbasis kecerdasan buatan.

Kata kunci: Keamanan siber, *Wazuh, LogRhythm, Pyramid of Pain, SIEM, VirusTotal, CrowdStrike Falcon*