ABSTRAK

Perkembangan teknologi informasi yang pesat telah meningkatkan kebutuhan akan sistem keamanan siber yang mampu mendeteksi dan menganalisis ancaman secara efektif. Salah satu pendekatan yang banyak digunakan saat ini adalah integrasi sistem deteksi intrusi berbasis host (HIDS) dengan kerangka kerja analisis ancaman seperti MITRE ATT&CK. Namun, dalam proses analisis terhadap log dan insiden yang tercatat menggunakan alat seperti Wazuh dan Elasticsearch, ditemukan bahwa alarm atau rule yang dihasilkan belum sepenuhnya terhubung secara langsung dengan framework MITRE ATT&CK. Hal ini menyulitkan proses identifikasi taktik dan teknik serangan karena kurangnya pemetaan otomatis antara insiden yang terdeteksi dan struktur taksonomi dalam MITRE ATT&CK. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan solusi berupa rule khusus yang secara otomatis mengaitkan setiap alarm atau insiden yang muncul dengan taktik dan teknik yang sesuai di dalam MITRE ATT&CK. Lingkungan uji coba dibangun dengan mengintegrasikan Wazuh sebagai HIDS dan Elasticsearch sebagai sistem penyimpanan serta analisis log. Melalui pendekatan ini, insiden yang terdeteksi dapat diklasifikasikan secara real-time dan kontekstual, sehingga proses analisis menjadi lebih cepat, akurat, dan mendalam. Hasil dari penelitian menunjukkan bahwa pemetaan otomatis ini mampu meningkatkan efektivitas dalam mendeteksi serta merespons insiden keamanan.

Kata kunci: *Wazuh, MITRE ATT&CK, Elasticsearch, Keamanan Siber, Rule Mapping, Deteksi Ancaman*.