INTISARI

Serangan siber yang semakin canggih karena perkembangan teknologi yang masif, menyebabkan perusahaan harus selalu memperbarui pengetahuan mengenai informasi terbaru serangan siber. Informasi yang terus berkembang tersebut memerlukan sebuah sistem manajemen insiden yang dapat mengatasi peningkatan jumlah kompleksitas insiden serangan siber dengan mengidentifikasi, analisis, dan mendapatkan pemahaman mengenai ancaman yang terjadi pada suatu sistem. Penelitian ini mengusulkan pengembangan sistem otomatisasi manajemen insiden menggunakan platform n8n pada aplikasi manajemen tiket Zammad. Informasi analisis yang diberikan akan berasal dari data korelasi *events* yang dimiliki aplikasi MISP. Sistem akan menggunakan pendekatan korelasi *events* dengan penerapan kerangka analisis *diamond model* pada fitur pencarian *threat actor*. Sistem yang dibangun berhasil menjalankan fungsi setiap fitur sesuai dengan hasil yang diharapkan. Hasil pengujian kinerja sistem korelasi adalah waktu pemrosesan data akan meningkat sebesar 74,2 % ketika ukuran data meningkat 1,6 kali lipat. Penelitian ini diharapkan dapat meningkatan kemampuan sistem manajemen tiket Zammad dalam memberikan korelasi insiden berdasarkan informasi mengenai temuan ancaman siber.

Kata Kunci: Manajemen Insiden, Zammad, n8n, MISP, *Diamond Model*.

ABSTRACT

Cyber attacks are increasingly sophisticated due to massive technological developments, causing companies to constantly update their knowledge about the latest information on cyber attacks. This growing information requires an incident management system that can overcome the increasing complexity of cyber attack incidents by identifying, analyzing, and understanding the threats on a system. This research proposes developing an incident management automation system using the n8n platform on the Zammad ticket management application. The analysis information will come from event correlation data owned by the MISP application. The system will use the event correlation approach by applying the diamond model analysis framework to the threat actor search feature. The system built successfully performs the functions of each feature by the expected results. The result of testing the performance of the correlation system is that the data processing time will increase by 74.2% when the data size increases 1.6 times. This research is expected to improve the ability of the Zammad ticket management system to provide incident correlation based on information about cyber threat findings.

Keywords: Incident Management, Zammad, n8n, MISP, Diamond Model.