UNIVERSITAS
GADJAH MADA

Perancangan Pipeline Otomasi Security Operations Center untuk Mitigasi Alert pada Wazuh
Josua Adhi Candra Nugroho, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Security operations center menghadapi tantangan *alert fatigue* ketika volume peringatan yang harus ditinjau analis lebih besar daripada jumlah kejadian yang benar-benar perlu ditindaklanjuti. Kondisi tersebut dapat memperlambat proses triase dan meningkatkan risiko terlewatnya ancaman nyata. Penelitian ini bertujuan merancang dan mengevaluasi *pipeline* otomasi SOC berbasis *security orchestration, automation, and response* (SOAR) untuk mendukung penyaringan *alert*, pembentukan *case*, analisis awal, dan dokumentasi insiden. Metode yang digunakan adalah membangun alur terintegrasi yang menghubungkan Wazuh, Python, MongoDB, n8n, AI *agent*, dan Jira. Model *machine learning* yang diuji meliputi *random forest*, XGBoost, dan *isolation forest*, dengan *random forest* sebagai model utama. *Dataset* yang digunakan mencakup *Wazuh Alerts Dataset*, AIT-ADS, dan *dataset* sintetis untuk pengujian alur serta evaluasi diagnosis AI *agent*. Hasil penelitian menunjukkan bahwa model mampu mempertahankan performa klasifikasi yang baik pada data uji terpisah, sedangkan pengujian *end-to-end* menunjukkan bahwa *pipeline* dapat mereduksi volume *alert* menjadi jumlah *case* dan tiket yang lebih ringkas. Integrasi AI *agent* juga mampu menghasilkan diagnosis dan rekomendasi awal, meskipun masih terdapat keterbatasan pada kesesuaian diagnosis terhadap konteks *log*. Dengan demikian, *pipeline* yang dikembangkan dapat mendukung efisiensi triase SOC, tetapi masih memerlukan pengayaan konteks dan validasi analis keamanan.

Kata kunci : *alert fatigue*, SOC, *pipeline*, SOAR, AI *agent*

UNIVERSITAS
GADJAH MADA

Perancangan Pipeline Otomasi Security Operations Center untuk Mitigasi Alert pada Wazuh
Josua Adhi Candra Nugroho, Dani Adhipta, S.Si., M.T.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

Security operations center (SOC) faces the challenge of alert fatigue when the volume of alerts reviewed by analysts exceeds the number of events that actually require follow-up. This condition can slow down the triage process and increase the risk of missing real threats. This study aims to design and evaluate an SOC automation pipeline based on security orchestration, automation, and response (SOAR) to support alert filtering, case formation, initial analysis, and incident documentation. The method used in this study is the development of an integrated workflow that connects Wazuh, Python, MongoDB, n8n, AI agent, and Jira. The tested machine learning models include random forest, XGBoost, and isolation forest, with random forest selected as the main model. The datasets used include the Wazuh Alerts Dataset, AIT-ADS, and a synthetic dataset for workflow testing and AI agent diagnosis evaluation. The results show that the model was able to maintain good classification performance on a separate test set, while the end-to-end test showed that the pipeline could reduce alert volume into a more concise number of cases and tickets. The AI agent integration was also able to generate initial diagnoses and recommendations, although limitations remained in the alignment of diagnoses with log context. Therefore, the developed pipeline can support SOC triage efficiency, but still requires context enrichment and validation by security analysts.

Keywords : *alert fatigue*, SOC, *pipeline*, SOAR, AI *agent*