ABSTRAK

Intrusion Detection System (IDS) merupakan salah satu mekanisme penting dalam menjaga keamanan jaringan. IDS terbagi menjadi dua berdasarkan cara deteksinya, yaitu *signature* dan *anomaly.* Metode *signature* memiliki kelemahan dalam mendeteksi serangan yang tidak diketahui, sedangkan metode *anomaly* dapat mendeteksi serangan yang tidak diketahui tetapi cenderung menghasilkan *false positive* yang tinggi. Penelitian ini mengusulkan model hibrida yang menggabungkan Suricata sebagai komponen *signature* dan *Isolation Forest* sebagai komponen *anomaly.* Model hibrida memungkinkan deteksi serangan dengan pola tidak diketahui yang tidak dapat ditangani oleh metode *signature* secara mandiri. Untuk membatasi *false positive* yang dihasilkan oleh komponen *anomaly,* penelitian ini mengusulkan mekanisme tambahan berupa *gating* menggunakan *watchlist* pada level *decision* akhir sistem. Pengujian pada penelitian dilakukan terhadap dataset CIC-IDS2017 dengan dua skenario utama, yaitu *known attack* dan *unknown attack*. Tanpa *gating*, model hibrida menghasilkan nilai *false positive* yang cukup tinggi. Dengan mekanisme *watchlist* pada *decision*, model hibrida berhasil membatasi FPR dari 34,74% menjadi 0,063% pada skenario *known attack*, serta membatasi FPR dari 33,82% menjadi 0,486% pada skenario *unknown attack*. Selain itu, model juga memiliki performa deteksi serangan yang lebih baik jika dibandingkan model mandiri. Pada skenario *known attack,* performa deteksi serangan meningkat sebesar 1,58% jika dibandingkan dengan Suricata. Pada skenario *unknown attack,* serangan yang gagal dideteksi oleh Suricata berhasil dideteksi oleh model hibrida dengan nilai mencapai 80%. Kemampuan tersebut datang dengan konsekuensi peningkatan sumber daya komputasi yang cukup besar.

***Kata Kunci**: anomaly, Intrusion Detection System, hibrida, signature, unknown attack*