SISTEM MONITORING KEAMANAN SERVER DENGAN SURICATA DI DISKOMINFOS PROVINSI BALI

I. W. Dimas Wirahadi[1], I. G. S. Astawa[2], dan I.G.N.A.C.Putra[3]

ABSTRAK

Implementasi sistem monitoring keamanan server menggunakan Suricata di Dinas Komunikasi dan Informatika Provinsi Bali. Suricata merupakan IDS/IPS (Intrusion Detection System/Intrusion Prevention System) yang kuat dan fleksibel yang dapat mendeteksi ancaman keamanan jaringan secara real-time. Penelitian ini membahas langkah-langkah penerapan Suricata untuk mendeteksi serangan dan ancaman potensial terhadap server di lingkungan organisasi. Metode ini melibatkan konfigurasi Suricata, pemantauan lalu lintas jaringan, dan analisis log untuk mengidentifikasi potensi ancaman keamanan. Hasil penelitian ini diharapkan dapat meningkatkan tingkat keamanan server di Dinas Komunikasi, Informatika, dan Statistika Provinsi Bali dan memberikan wawasan tentang efektivitas Suricata sebagai alat pemantauan keamanan jaringan server..

Kata kunci : Suricata, IDS/IPS, keamanan jaringan, monitoring server, analisis log.

ABSTRACT

Implementation of a server security monitoring system using Suricata was carried out at the Bali Provincial Communication and Informatics Office. Suricata is a powerful and flexible IDS/IPS (Intrusion Detection System/Intrusion Prevention System) capable of detecting network security threats in real time. This study discusses the implementation steps of Suricata to detect attacks and potential threats against servers within the organizational environment. The method involves configuring Suricata, monitoring network traffic, and analyzing logs to identify potential security risks. The results of this research are expected to improve the level of server security at the Bali Provincial Office of Communication, Informatics, and Statistics and provide insights into the effectiveness of Suricata as a server network security monitoring tool.

Keywords: Suricata, IDS/IPS, network security, server monitoring, log analysis.

1. PENDAHULUAN

Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali (Diskominfos Bali) merupakan lembaga pemerintah yang memiliki peran penting dalam pengelolaan informasi publik dan layanan digital daerah (Diskominfos Provinsi Bali, 2023). Sebagai pusat layanan data dan informasi, Diskominfos Bali mengelola berbagai server yang menyimpan data sensitif dan aplikasi penting bagi masyarakat

[1] *Program StudiInformatika, FakultasMatematika dan Ilmu Pengetahuan Alam, UniversitasUdayana,Denpasar-Indonesia, iwayandimas20@gmail.com*
[2] *Program StudiInformatika, FakultasMatematika dan Ilmu Pengetahuan Alam, UniversitasUdayana , Denpasar-Indonesia, santi.astawa@unud.ac.id.*
[3] *Program StudiInformatika, FakultasMatematika dan Ilmu Pengetahuan Alam, UniversitasUdayana , Denpasar-Indonesia, anom.cp@unud.ac.id.*
Submitted: 25 Oktober 2025 *Revised: 1 November 2025* *Accepted: 7 November 2025*

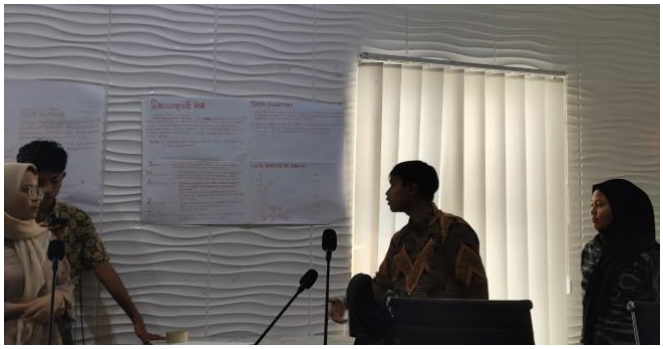
maupun instansi pemerintah. Tingginya ketergantungan terhadap layanan digital menuntut adanya sistem keamanan yang andal untuk melindungi server dari ancaman serangan siber yang semakin kompleks dan bervariasi. Ancaman keamanan jaringan seperti Distributed Denial of Service (DDoS), SQL Injection, Cross Site Scripting (XSS), dan pemindaian port dapat menyebabkan gangguan layanan, kebocoran data, serta kerugian operasional (Stiawan et al., 2019). Kondisi ini menuntut strategi pengamanan proaktif melalui sistem monitoring yang mampu mendeteksi serangan secara real-time (Ninawe & Meshram, 2018). Salah satu solusi yang efektif dalam menghadapi tantangan ini adalah penerapan Intrusion Detection System/Intrusion Prevention System (IDS/IPS). Suricata merupakan IDS/IPS open source yang memiliki kemampuan mendeteksi, menganalisis, serta mencegah lalu lintas jaringan berbahaya. Keunggulan Suricata terletak pada fleksibilitas konfigurasi, kemampuan membaca berbagai protokol, serta dukungan real-time logging yang memudahkan analisis keamanan (OISF, 2023). Dengan menerapkan Suricata di lingkungan Diskominfos Bali, diharapkan dapat meningkatkan ketahanan sistem server, mendukung kelancaran layanan publik, serta memberikan perlindungan lebih baik terhadap data dan infrastruktur digital pemerintah daerah..

2. METODE PELAKSANAAN

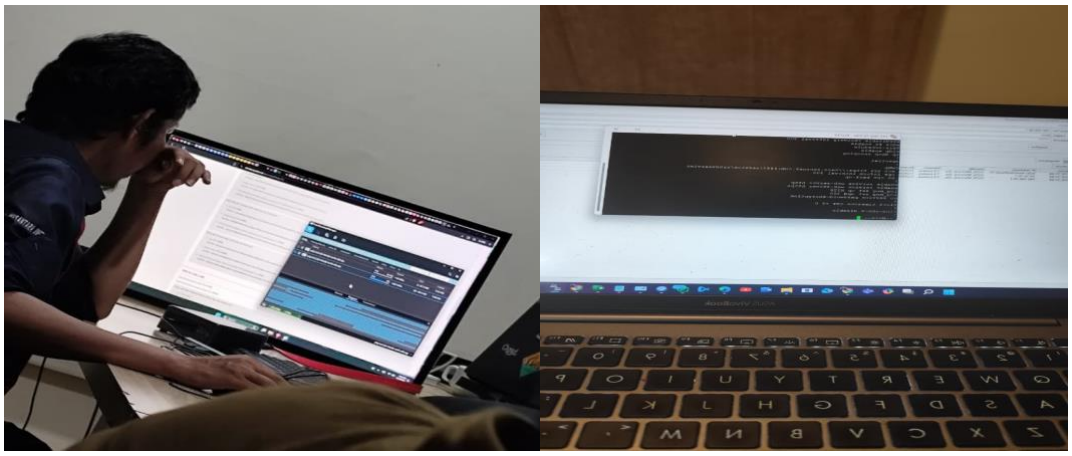
Proses pelaksanaan kegiatan pengabdian ini melibatkan serangkaian tahap yang dirancang secara sistematis untuk memastikan sistem monitoring keamanan server yang dihasilkan benar-benar dapat menjawab kebutuhan operasional di Diskominfos Provinsi Bali. Tahap awal dimulai dengan identifikasi kebutuhan dan analisis situasi yang dilakukan melalui diskusi bersama pihak-pihak terkait, khususnya staf bidang persandian yang memiliki tanggung jawab dalam pengelolaan server yang ditunjukkan oleh gambar 2.1. Pada tahap ini dilakukan pemetaan permasalahan utama yang dihadapi, antara lain tingginya potensi ancaman serangan siber, kebutuhan akan sistem deteksi dini, serta keterbatasan mekanisme monitoring manual yang masih digunakan. Hasil analisis kebutuhan tersebut kemudian menjadi pedoman dalam merancang rancangan awal sistem monitoring berbasis Suricata.

Gambar 2. 1 Diskusi Dengan Pihak Terkait

Tahap selanjutnya adalah perumusan solusi dengan melakukan instalasi dan konfigurasi Suricata pada server utama yang digunakan sebagai pusat monitoring yang ditunjukkan oleh gambar 2.2. pada gmabar 2.3 dibawah dilakukan konfigurasi sistem oleh pihak terkait, Konfigurasi ini mencakup penyesuaian aturan (rules) Suricata, integrasi dengan sistem logging, serta pengaturan agar Suricata mampu mendeteksi berbagai jenis serangan seperti port scanning, DDoS, maupun eksploitasi aplikasi berbasis web. Implementasi dilakukan secara bertahap agar proses pengembangan sistem lebih mudah diawasi dan apabila terjadi kendala teknis dapat segera diatasi. Selain itu, dilakukan pula pengujian internal untuk memastikan bahwa sistem dapat berjalan stabil di lingkungan jaringan Diskominfos Bali.



Gambar 2. 2 Perancangan Sistem dan Perumusan Solusi



Gambar 2. 3 Konfigurasi dan Instalasi System

Setelah tahap implementasi teknis, dilakukan kegiatan sosialisasi kepada pegawai dan staf teknis Diskominfos Bali. Sosialisasi ini bertujuan agar pengguna memiliki pemahaman yang memadai mengenai fungsi dasar sistem monitoring, cara membaca log, serta langkah tindak lanjut jika ditemukan aktivitas mencurigakan. Edukasi ini dilaksanakan melalui sesi diskusi, demonstrasi langsung penggunaan dashboard Suricata, serta simulasi serangan untuk menguji respons sistem. Dengan pendekatan ini, diharapkan staf dapat lebih proaktif dalam memanfaatkan sistem, bukan hanya sebagai alat deteksi, tetapi juga sebagai dukungan dalam pengambilan keputusan terkait keamanan jaringan.

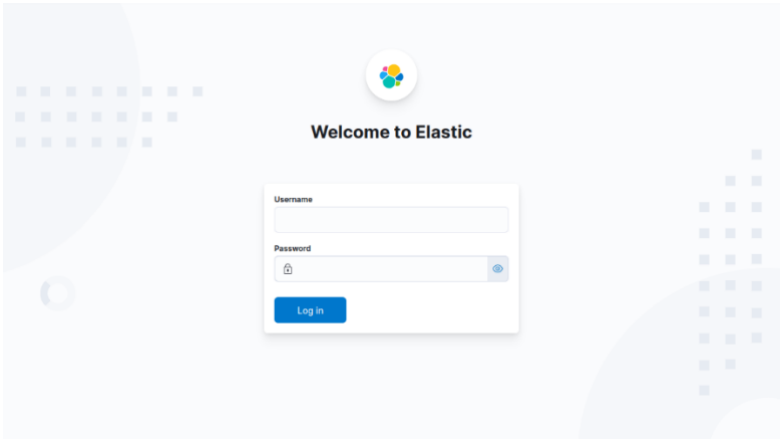
Gambar 2. 5 Pemaparan Project dan Sosialisasi Sistem

Tahap akhir dari metode pelaksanaan adalah evaluasi dan tindak lanjut. Evaluasi dilakukan dengan melibatkan pimpinan dan pembimbing lapangan untuk menilai efektivitas sistem, mencatat kekurangan, serta merumuskan rekomendasi pengembangan lebih lanjut. Evaluasi mencakup kecepatan sistem dalam mendeteksi serangan, keakuratan log yang dihasilkan, serta kemudahan penggunaan antarmuka monitoring. Hasil evaluasi ini digunakan sebagai masukan bagi perbaikan sistem ke depan, termasuk rencana penambahan fitur otomatisasi laporan, integrasi dengan teknologi keamanan lain, serta pengembangan modul pelatihan berkelanjutan. Metode pengabdian ini dirancang secara sistematis dengan tahapan analisis kebutuhan, instalasi Suricata, konfigurasi rules, dan sosialisasi kepada staf. Pendekatan ini selaras dengan penelitian yang menekankan pentingnya perancangan IDS berbasis Suricata yang terintegrasi dengan sistem logging agar dapat mendukung deteksi cepat (Guo et al., 2022; Pinto et al., 2023). Melalui proses ini, diharapkan sistem monitoring berbasis Suricata dapat terus dikembangkan agar semakin efektif dalam meningkatkan keamanan server dan jaringan di Diskominfos Provinsi Bali.

Gambar 2. 4 Tahap Evaluasi Sistem dan pemaparan hasil Project Kepada Staff dan Pimpinan Secara Online

3. HASIL DAN PEMBAHASAN

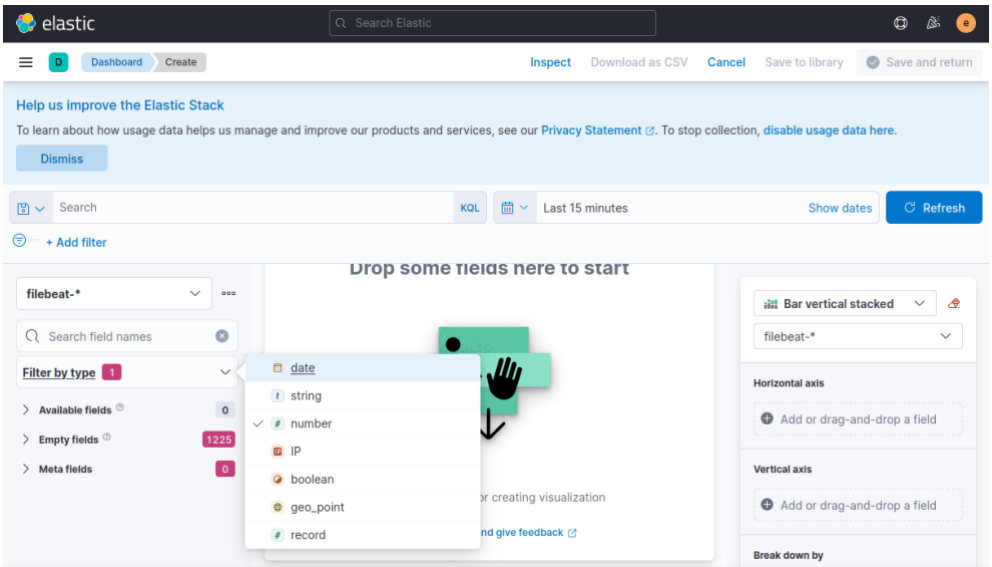
Hasil dari kegiatan pengabdian ini adalah terbangunnya sebuah sistem monitoring keamanan server berbasis Suricata yang dapat digunakan di lingkungan Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali. Sistem ini dikembangkan dengan tujuan untuk membantu staf bidang persandian dalam melakukan pemantauan lalu lintas jaringan secara real-time serta mendeteksi potensi ancaman yang dapat membahayakan server. Implementasi sistem dilakukan melalui beberapa tahap, mulai dari instalasi dan konfigurasi Suricata, pengujian sistem pada jaringan lokal, hingga penyusunan antarmuka monitoring yang memudahkan analisis keamanan oleh operator.



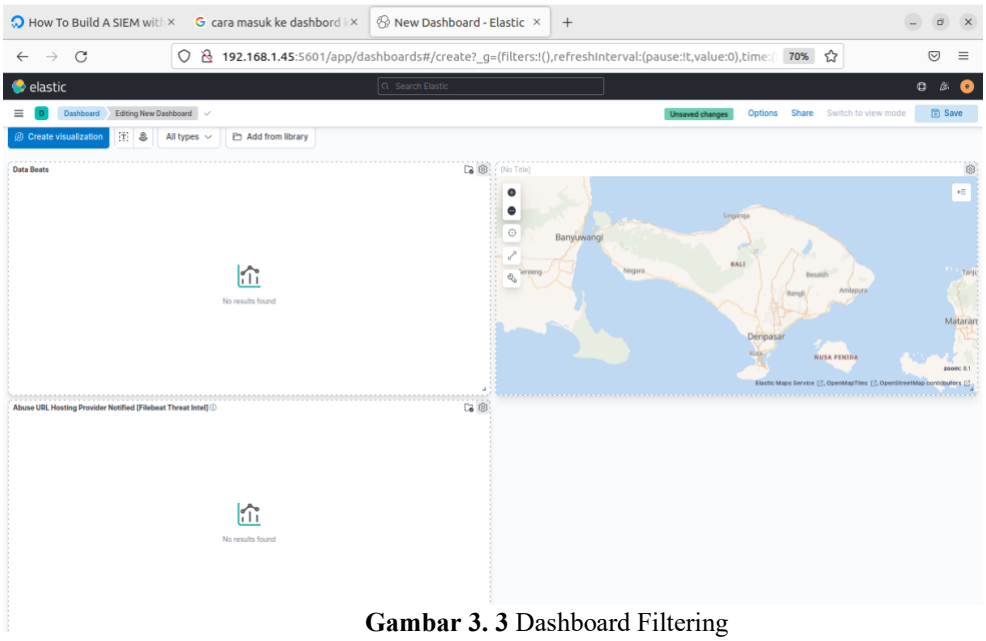
Gambar 3. 1 Halaman Login

Secara teknis, sistem ini memiliki beberapa komponen utama. Pertama, halaman login yang ditunjukkan Gambar 1, berfungsi sebagai gerbang masuk bagi pengguna yang berwenang. Fitur autentikasi ini memastikan bahwa hanya staf tertentu yang dapat mengakses dashboard monitoring sehingga menjaga kerahasiaan data.

Kedua, sistem dilengkapi dengan dashboard monitoring yang menyajikan informasi trafik jaringan dan aktivitas server secara menyeluruh. Dashboard ini menampilkan data lalu lintas yang masuk dan keluar, status server yang diawasi, serta ringkasan ancaman yang terdeteksi oleh Suricata. Dengan tampilan yang sederhana namun informatif, dashboard mempermudah pengguna dalam memahami kondisi jaringan tanpa harus membaca log teknis secara detail yang ditunjukkan oleh Gambar 3.2.

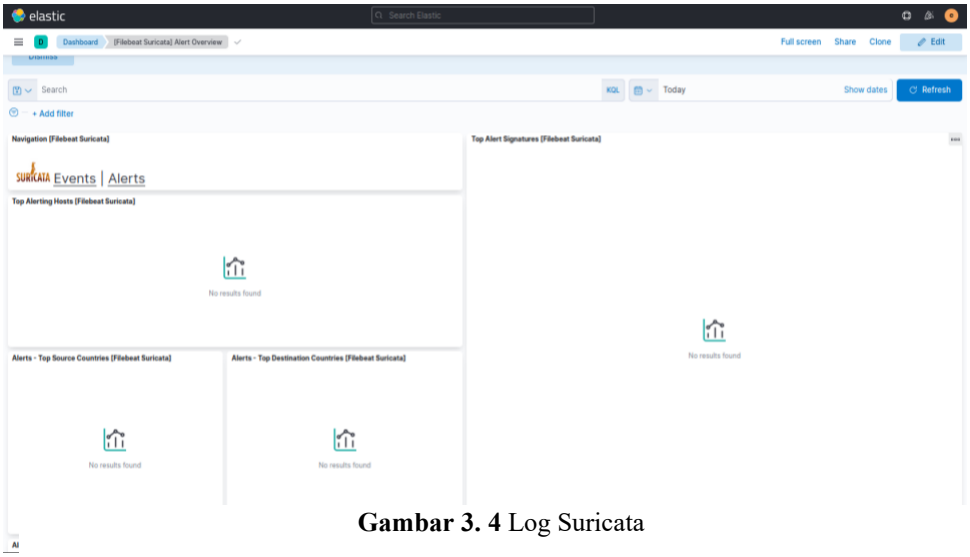


Ketiga, terdapat fitur filtering dashboard yang ditunjukkan oleh gambar 3.3 memungkinkan pengguna menyaring data sesuai kebutuhan analisis. Melalui fitur ini, operator dapat memfokuskan pemantauan pada jenis protokol tertentu, alamat IP spesifik, atau kategori serangan yang ingin ditelusuri lebih dalam. Fitur ini memberikan fleksibilitas tinggi bagi pengguna untuk menyesuaikan tampilan data dengan kebutuhan operasional.



Gambar 3. 3 Dashboard Filtering

Keempat, sistem menyajikan log aktivitas Suricata yang mencatat seluruh peristiwa keamanan secara rinci. Setiap serangan atau aktivitas mencurigakan yang terdeteksi akan tercatat dalam log baik dalam bentuk teks maupun grafik. Log ini menjadi sumber informasi penting dalam melakukan analisis forensik keamanan, karena dapat menunjukkan jenis ancaman, sumber serangan, serta waktu kejadian. Informasi yang terdokumentasi secara real-time memungkinkan staf melakukan langkah respons lebih cepat dan terukur.



Gambar 3. 4 Log Suricata

Dari hasil perancangan, sistem monitoring yang dibangun mampu menampilkan informasi keamanan jaringan secara real-time dan mencatat berbagai aktivitas penting, termasuk deteksi serangan seperti port scanning, percobaan akses ilegal, dan serangan berbasis protokol. Rancangan sistem ini menunjukkan bahwa Suricata dapat diintegrasikan dengan baik sebagai komponen utama dalam monitoring server, dengan dukungan antarmuka dashboard, fitur filter, serta pencatatan log aktivitas yang memudahkan analisis keamanan. Hasil rancangan sistem menunjukkan bahwa Suricata dapat mendeteksi berbagai ancaman seperti port scanning, akses ilegal, hingga serangan berbasis protokol. Hal ini sejalan dengan penelitian yang menyatakan Suricata mampu memberikan *alert* yang efektif berdasarkan indikator kompromi (Raharjo & Salman, 2023). Hasil rancangan ini diharapkan dapat menjadi solusi awal dalam meningkatkan ketahanan server di lingkungan Diskominfos Bali dan dapat dikembangkan lebih lanjut untuk mendukung kebutuhan operasional yang lebih luas.

4. KESIMPULAN

Kegiatan pengabdian masyarakat yang dilaksanakan di Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali berhasil menghasilkan sebuah sistem monitoring keamanan server berbasis Suricata. Sistem ini dirancang untuk membantu staf dalam mendeteksi dan menganalisis ancaman jaringan secara real-time, sehingga dapat meningkatkan ketahanan server dari potensi serangan siber. Hasil perancangan menunjukkan bahwa Suricata mampu diintegrasikan dengan baik ke dalam lingkungan server instansi, dengan dukungan antarmuka dashboard, fitur filtering, serta log aktivitas yang komprehensif. Selain memberikan solusi teknis, kegiatan ini juga berdampak positif dalam peningkatan pengetahuan dan keterampilan staf melalui kegiatan sosialisasi serta uji coba sistem. Dengan adanya sistem ini, Diskominfos Bali memiliki sarana pendukung yang lebih andal dalam melakukan monitoring dan respons terhadap ancaman keamanan. Meskipun masih terdapat ruang untuk pengembangan, seperti integrasi dengan sistem keamanan lain dan penyempurnaan fitur otomatisasi laporan, hasil pengabdian ini telah memberikan kontribusi nyata dalam memperkuat infrastruktur keamanan informasi di lingkungan pemerintah daerah. Ke depan, diharapkan sistem ini dapat dikembangkan secara berkelanjutan dan menjadi model penerapan IDS/IPS yang dapat diadopsi oleh instansi pemerintah lain di Indonesia. Kegiatan pengabdian ini membuktikan bahwa Suricata dapat diimplementasikan sebagai sistem monitoring keamanan server yang efektif di lingkungan instansi pemerintah. Hasil rancangan sesuai dengan penelitian terdahulu yang menekankan efektivitas IDS/IPS berbasis Suricata (Stiawan et al., 2019; Rahman & Pratama, 2020). Selain itu, pengembangan sistem ke depan dapat diarahkan pada integrasi dengan kecerdasan buatan sebagaimana tren terbaru pada sistem IDS (Pinto et al., 2023; Sharma, 2024).

DAFTAR PUSTAKA

Aho, A. V., & Corasick, M. J. (1975). Efficient string matching: An aid to bibliographic search. Communications of the ACM, 18(6), 333–340. https://doi.org/10.1145/360825.360855

Diskominfos Provinsi Bali. (2023). Tugas dan Fungsi Diskominfos Pemerintah Provinsi Bali. Diakses dari: https://diskominfos.baliprov.go.id/tugas-pokok-dan-fungsi/

Guo, J., Guo, H., & Zhang, Z. (2022). Research on High Performance Intrusion Prevention System Based on Suricata. Highlights in Science, Engineering and Technology AIEA, 7, 238.

Hoover, C. (2022). Comparative study of Snort 3 and Suricata Intrusion Detection Systems. Computer Science and Computer Engineering Undergraduate Honors Theses.

Ninawe, S. P., & Meshram, B. B. (2018). Network Intrusion Prevention System (NIPS) using open-source tools. International Journal of Advanced Research in Computer Science, 9(2), 142–148. https://doi.org/10.26483/ijarcs.v9i2.5835

Open Information Security Foundation (OISF). (2023). Suricata Documentation. Retrieved from https://suricata.readthedocs.io

Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. Sensors, 23(5), 2415. https://doi.org/10.3390/s23052415

Rahman, A., & Pratama, B. (2020). Analisis implementasi intrusion detection system Suricata untuk keamanan jaringan. Jurnal Teknologi Informasi dan Ilmu Komputer, 7(2), 145–152. https://doi.org/10.25126/jtiik.202072345

Raharjo, D. H. K., & Salman, M. (2023). Analyzing Suricata alert detection performance issues based on active indicator of compromise rules. Jurnal Teknik Informatika (JUTIF), 4(3), 601–610. https://doi.org/10.52436/1.jutif.2023.4.3.1013

Sharma, V. (2024). Artificial intelligence based intrusion detection system. ITM Web of Conferences (ICMAETM). https://doi.org/10.1051/itmconf/202425601018

Stiawan, D., Idris, M. Y., & Abdullah, A. H. (2019). Intrusion detection and prevention system using Suricata: Design and implementation. International Journal of Computer Applications, 182(4), 23–29. https://doi.org/10.5120/ijca2019918344

Tahir, M. (2024). Development of network security using a Suricata-based intrusion prevention system. Innovatics.