ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI SISTEM DETEKSI SERANGAN PADA JARINGAN ENDPOINT

TUGAS AKHIR

diajukan oleh:

Nama : Muhammad Abdul Halim

NIM : 22.01.4875

PROGRAM DIPLOMA

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI SISTEM DETEKSI SERANGAN PADA JARINGAN ENDPOINT

TUGAS AKHIR

Diajukan untuk memenuhi salah satu syarat mencapai gelar Ahli Madya Komputer Program Diploma – Program Studi Teknik Informatika

diajukan oleh

Nama : Muhammad Abdul Halim

NIM : 22.01.4875

PROGRAM DIPLOMA

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

TUGAS AKHIR

ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI SISTEM DETEKSI SERANGAN PADA JARINGAN ENDPOINT

yang dipersiapkan dan disusun oleh

Muhammad Abdul Halim

22.01.4875

Telah disetujui oleh Dosen Pembimbing Tugas Akhir

pada tanggal 7 Juli 2025

Dosen Pembimbing,

Pramedhita Ferdiansyah, M.Kom

NIK. 190302409

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI SISTEM DETEKSI SERANGAN PADA JARINGAN ENDPOINT

yang disusun dan diajukan oleh

Muhammad Abdul Halim

22.01.4875

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Nila Feby Puspitasari, S.Kom., M.Cs. NIK. 190302161	
Ali Mustopa, S.Kom., M.Kom. NIK. 190302192	

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya komputer
Tanggal 21 Juli 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Abdul Halim
NIM : 22.01.4875

Menyatakan bahwa Tugas Akhir dengan judul berikut:

Analisis Kinerja Wazuh dan Suricata Sebagai Sistem Deteksi Serangan Pada Jaringan Endpoint

Dosen Pembimbing : Pramudhita Ferdiansyah, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 Juli 2025

Yang Menyatakan,

Muhammad Abdul Halim

HALAMAN PERSEMBAHAN

Puji syukur kehadirat Allah SWT atas limpahan Rahmat serta Karunia-Nya sehingga saya dapat menyelesaikan tugas akhir ini.

Dengan segala rasa hormat dan rasa sayang, saya persembahkan Tugas Akhir ini untuk kedua orang tua saya, bapak Hamidi Prasetya dan Ibu Partini yang sangat saya sayangi. Terima kasih atas segala limpahan doa, dukungan moral dan materi, serta pengorbanan yang sangat luar biasa untuk mendukung langkah dalam mengejar mimpi-mimpi.

Kakak tercinta Rohmah Susana Eka Putri dan Azis Arifin, serta Keponakan Tercinta Arsyila Zakiya Arifin, terimakasih telah memberikan semangat, mendukung, mendoakan dan memberikan kecerian dalam setiap hari saya.

Terima kasih juga saya ucapkan untuk sahabat-sahabat saya yang telah menjadi sahabat terbaik saya selama di lingkungan perkuliahan, yang selalu memberikan dukungan, dorongan, dan selalu membantu dalam setiap kesulitan yang saya hadapi.

Terima kasih untuk semua yang telah membantu saya selama ini dalam meraih cita-cita.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, yang telah melimpahkan rahmat, hidayah, serta karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir ini dengan lancar. Tugas akhir ini disusun untuk memenuhi salah satu syarat kelulusan Program Diploma 3 pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Selain itu penulis dengan segala kerendahan hati ingin menyampaikan rasa terima kasih kepada semua pihak yang telah berjasa memberikan dukungan dan bantuan untuk menyelesaikan laporan tugas akhir ini. Untuk itu penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM, selaku Rektor Universitas Amikom Yogyakarta
2. Ibu Prof. Dr. Kusrini, M.Kom. selaku Dekan Program Fakultas Ilmu Komputer
3. Bapak Barka Satya, M.Kom, selaku Ketua Program Studi D3 Teknik Informatika Universitas Amikom Yogyakarta.
4. Bapak Pramudhita Ferdiansyah, M.Kom, selaku dosen pembimbing yang memberikan arahan, saran, dan motivasi terhadap penulis
5. Kedua orang tua, keluarga besar, dan teman-teman tercinta yang memberikan semangat dan doa kepada penulis.

Yogyakarta, 7 Juli 2025

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

SIEM	*Security Information and Event Management*
IDS	*Intrusion Detection System*
HIDS	*Host Based Intrusion Detection System*
VM	*Virtual Machine*
VPS	*Virtual Private Server*
API	*Application Programing Interface*
DDoS	*Distributed Denial of Service*
SQL	*Structured Query Language*
SSD	*Solid State Drive*
RAM	*Random Access Memory*
vCPU	*Virtual Central Unit Processing*
JSON	*JavaScript Object Notation*
SPDLC	*Security Policy Development Life Cycle*

DAFTAR ISTILAH

Rule	Aturan atau intruksi aksi ketika sistem mengidentifikasi pola potensi ancaman dan serangan dalam jaringan.
Signature	Pola yang dianalisis dalam paket atau lalu lintas jaringan.
False Positif	Bukan serangan, terdeteksi.
True Positif	Benar Serangan, Terdeteksi.
Event	Catatan berisi informasi peristiwa atau insiden pada sistem.
Log	Kumpulan Event.
Alert	Laporan Insiden pada Sistem.
Threshold	Nilai minimum atau batas yang ditetapkan untuk suatu kondisi atau kriteria, yang jika dilampaui atau dicapai akan memicu tindakan tertentu.
Tools	Alat untuk membantu suatu kegiatan.

INTISARI

Endpoint merupakan komponen yang rentan dan sering menjadi sasaran berbagai jenis serangan siber, mulai dari perusakan sistem hingga pencurian data penting. Untuk menjaga keamanan *endpoint*, dibutuhkan pemantauan. Namun, pemantauan secara konvensional seperti membaca log host memakan waktu dan sumber daya, sehingga serangan berpotensi tidak terdeteksi secara langsung. Untuk memastikan keamanan endpoint, tujuan penelitian adalah dengan mengembangkan sistem informasi keamanan, manajemen *event* dan sistem deteksi sehingga terdapat respon cepat ketika terjadi insiden.

Penelitian ini menggunakan pendekatan SPDLC (*Security Policy Development Life Cycle*) untuk membangun sistem keamanan jaringan. Wazuh sebagai SIEM (*Security Information and Event Management*) diimplementasikan untuk mengelola log dari endpoint dan mengirimkan alert ke API Telegram secara real-time. Wazuh mendeteksi anomali dengan menganalisis log host berdasarkan rule bawaan. Sistem juga dilengkapi Suricata sebagai IDS (Intrusion Detection System) yang memantau lalu lintas jaringan dan mencocokkannya dengan signature yang ada, untuk mendeteksi serangan seperti Port Scanning, DDoS, Brute Force, dan SQL Injection.

Pengujian dilakukan dengan menyerang server target yang menjalankan aplikasi web menggunakan 4 jenis serangan tersebut. Hasil pada pengujian menunjukan, serangan dapat terdeteksi dengan waktu dari mulai serangan dilakukan hingga alert keluar pada notifikasi telegram, adalah antara 1 detik hingga paling lama 7 detik. Hasil ini menunjukkan bahwa kinerja Wazuh dan Suricata dapat mendeteksi berbagai jenis serangan secara real-time dengan delay yang relatif singkat, sehingga membantu meningkatkan keamanan *endpoint*.

Kata kunci: Wazuh, Suricata, Endpoint, Keamanan, Jaringan

ABSTRACT

Endpoints are vulnerable components and are often targeted by various types of cyberattacks, ranging from system damage to the theft of critical data. Monitoring is required to maintain endpoint security. However, conventional monitoring methods such as reading host logs consume time and resources, potentially allowing attacks to go undetected immediately. To ensure endpoint security, the purpose of this research is to develop a security information system, event management, and detection system so that there is a quick response when an incident occurs.

This research uses the SPDLC (Security Policy Development Life Cycle) approach to build a network security system. Wazuh as a SIEM (Security Information and Event Management) is implemented to manage logs from endpoints and send alerts to the Telegram API in real time. Wazuh detects anomalies by analyzing host logs based on built-in rules. The system is also equipped with Suricata as an IDS (Intrusion Detection System) that monitors network traffic and matches it with existing signatures to detect attacks such as Port Scanning, DDoS, Brute Force, and SQL Injection.

Testing was carried out by attacking a target server running a web application using these four types of attacks. The results of the tests show that the attacks can be detected, with the time from when the attack starts until the alert appears on the Telegram notification being between 1 second and at most 7 seconds. These results indicate that the performance of Wazuh and Suricata can detect various types of attacks in real time with relatively short delays, thus helping to enhance endpoint security.

Keyword: *Wazuh, Suricata, Endpoint, Security, Network*