TUGAS AKHIR
SKEMA MAGANG

INTEGRASI THREAT INTELLIGENCE DALAM SIEM WAZUH UNTUK DETEKSI DINI MALWARE

SULHAEDIR

NIM : 225411113

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

TUGAS AKHIR
SKEMA MAGANG

INTEGRASI THREAT INTELLIGENCE DALAM SIEM WAZUH UNTUK DETEKSI DINI MALWARE

Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada
Program Sarjana
Program Studi Informatika
Fakultas Teknologi Informasi
Universitas Teknologi Digital Indonesia

Disusun Oleh
SULHAEDIR
NIM : 225411113

PROGRAM STUDI INFORMATIKA
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Integrasi Threat Intelligence dalam Sistem Wazuh untuk Deteksi Dini Serangan Malware
Nama	:	Sulhaedir
NIM	:	225411113
Program Studi	:	Informatika
Program	:	Sarjana
Semester	:	Genap
Tahun Akademik	:	2024/2025

Telah diperiksa dan disetujui untuk diujikan
di hadapan Dewan Penguji Tugas Akhir

Yogyakarta, 19 Januari 2025

Dosen Pembimbing,

Dr. L.N. Harnaningrum, S.Si., M.T.
NIDN : 0513057101

HALAMAN PENGESAHAN

INTEGRASI THREAT INTELLIGENCE DALAM SIEM WAZUH UNTUK DETEKSI DINI MALWARE

Telah dipertahankan di depan Dewan Penguji dan dinyatakan diterima untuk memenuhi sebagian persyaratan guna memperoleh

Gelar Strata Satu

Program Studi Informatika

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Yogyakarta, 10 Februari 2025

Dewan Penguji	NIDN	Tandatangan
1. Agung Budi Prasetyo, S. Kom., M.Kom. (Ketua)	0003087106	.....
2. Dr. L.N. Harnaningrum, S.Si, M.T. (Sekretaris)	0513057101	.....
3. M. Agung Nugroho, S.Kom., M.Kom. (Anggota)	0507078501	.....

Mengetahui

Ketua Program Studi Informatika

Dini Fakta Sari, S.T., M.T.

NIDN : 0507108401

PERNYATAAN KEASLIAN TUGAS AKHIR

Dengan ini saya menyatakan bahwa naskah Tugas Akhir ini belum pernah diajukan untuk memperoleh gelar Strata Satu di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Jakarta, 16 Januari 2025

Sulhaedir
NIM: 225411113

HALAMAN PERSEMBAHAN

Puji dan syukur saya panjatkan atas kehadiran Allah SWT, yang telah memberikan kesehatan, rahmat dan hidayah, sehingga saya dapat menyelesaikan tugas akhir ini sebagai syarat memperoleh gelar sarjana. Walaupun tugas akhir ini masih memiliki kekurangan dan jauh dari kata sempurna namun saya bangga dapat menyelesaikan nya dengan tepat waktu.

Tugas akhir ini saya persembahkan kepada orang orang yang selalu memberikan dukungan:

- Kedua orang tua saya yang selalu memberikan kasih sayang, doa yang tak pernah putus, dan dukungan yang tak ternilai sepanjang hidup saya.
- Istri dan putri saya yang menjadi sumber semangat, kasih sayang, dukungan yang tak pernah putus dan selalu memberikan dorongan sehingga saya bisa menyelesaikan studi saya.
- Dosen pembimbing Ibu Ningrum yang selalu memberikan ilmu, bimbingan, serta arahan yang berharga selama proses penyusunan tugas akhir ini
- Teman teman dari PT SSI (Nemo Security) yang menjadi teman diskusi dari awal penyusunan hingga selesainya tugas akhir saya.

PRAKATA

Puji dan syukur saya panjatkan atas kehadirat Allah SWT, karena berkat rahmat dan hidayahNya penyusunan tugas akhir yang berjudul "Integrasi *Threat Intelligence* dalam Sistem Wazuh untuk Deteksi Dini Serangan Malware" ini dapat diselesaikan guna memenuhi salah satu persyaratan dalam menyelesaikan pendidikan strata satu pada jurusan Informatika Universitas Teknologi Digital Indonesia Yogyakarta

Berbagai hambatan saya lalui dalam menyelesaikan tugas akhir ini. Berkat kehendak-Nyalah sehingga saya berhasil menyelesaikan penulisan tugas akhir ini. Oleh karena itu, dengan penuh kerendahan hati, pada kesempatan ini saya mengucapkan terima kasih kepada:

- Sri Redjeki, S.Si, M.Kom., Ph.D. Selaku rektor UTDI Yogyakarta
- Dr. L.N. Harnaningrum, S.Si., M.T. Selaku dosen pembimbing
- Bapak Nezim S.kom., M.Kom. Selaku direktur PT Sekuriti Siber Indonesia
- Semua pihak yang telah banyak membantu dalam penyusunan skripsi ini yang tidak bisa saya sebutkan semuanya.

INTISARI

Keamanan siber menjadi salah satu isu utama di era digital, terutama dalam mendeteksi dan mencegah ancaman malware. Penelitian ini bertujuan untuk mengintegrasikan platform *Threat Intelligence* Malware Bazaar dengan sistem Wazuh untuk meningkatkan kemampuan deteksi malware secara real-time. Proses integrasi memanfaatkan API yang disediakan oleh Malware Bazaar dan memanfaatkan fitur *File Integrity Monitoring (FIM)* yang terdapat pada Wazuh.

Penelitian dilakukan dengan tiga tahap utama: pengumpulan data hash malware dari *Malware Bazaar*, implementasi integrasi API pada Wazuh, dan pengujian kemampuan deteksi menggunakan beberapa sampel malware. Hasil penelitian menunjukkan bahwa sistem berhasil mendeteksi ancaman malware dengan akurasi mencapai 80%, khususnya untuk file yang memiliki hash yang terdaftar di database *Malware Bazaar.*

Kesimpulan dari penelitian ini adalah bahwa integrasi platform *Threat Intelligence open-source* seperti *Malware Bazaar* dengan sistem SIEM berbasis Wazuh dapat memberikan solusi yang efektif dan ekonomis untuk deteksi dini malware. Penelitian ini juga membuka peluang untuk pengembangan lebih lanjut, seperti integrasi dengan platform Threat Intelligence lainnya atau penambahan fitur otomatisasi pada proses mitigasi.

Kata Kunci: Malware, Wazuh, Monitoring, SIEM

ABSTRACT

Cybersecurity has become a critical issue in the digital era, particularly in detecting and preventing malware threats. This study aims to integrate the MalwareBazaar Threat Intelligence platform with the Wazuh system to enhance real-time malware detection capabilities. The integration process utilizes the API provided by MalwareBazaar and leverages the File Integrity Monitoring (FIM) feature available in Wazuh.

The research methodology consists of three main stages: collecting malware hash data from MalwareBazaar, implementing API integration into Wazuh, and testing detection capabilities using several malware examples. The results demonstrate that the system successfully detects malware threats with an accuracy of up to 80%, particularly for files whose hashes are listed in the MalwareBazaar database.

The study concludes that integrating open-source Threat Intelligence platforms like MalwareBazaar with Wazuh-based SIEM systems provides an effective and economical solution for early malware detection. This research also opens opportunities for further development, such as integration with other Threat Intelligence platforms or adding automation features for mitigation processes.

Keywords: Malware, Wazuh, SIEM

DAFTAR ISI

Hal

DAFTAR GAMBAR

DAFTAR TABEL