UNIVERSITAS
GADJAH MADA
**Rancang Bangun Sistem Otomatisasi Threat Hunting Untuk Analisis Sumber Serangan Menggunakan Wazuh
dengan Intergrasi VirusTotal dan MongoDB**
Gagat Wijaya, Dr. Ir. Ronald Adrian, S.T., M.Eng., IPM., ASEAN Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Ancaman siber yang semakin berkembang menuntut proses *Threat Hunting* dilakukan secara cepat dan efektif. Namun, proses analisis *security alert* masih banyak dilakukan secara manual sehingga memerlukan waktu yang relatif lama dalam mengidentifikasi sumber serangan. Penelitian ini bertujuan merancang dan membangun sistem otomatisasi *Threat Hunting* untuk analisis sumber serangan menggunakan Wazuh dengan integrasi VirusTotal dan MongoDB. Sistem dikembangkan menggunakan bahasa pemrograman Python dengan pendekatan modular. Wazuh digunakan sebagai sumber *security alert*, VirusTotal untuk analisis reputasi alamat IP publik, MongoDB sebagai media penyimpanan hasil analisis, serta Streamlit untuk menampilkan *dashboard monitoring* dan Reportlab untuk menghasilkan laporan dalam format PDF. Pengujian dilakukan menggunakan dua skenario, yaitu *replay* dataset PCAP dari Malware Traffic Analysis dan simulasi serangan *Brute Force* SSH menggunakan Kali Linux terhadap Ubuntu Desktop. Pengujian performa dilakukan sebanyak 30 kali melalui dua kali *replay* dataset untuk mengukur *Overall Latency*, VirusTotal API *Latency*, dan Internal *Processing Latency*. Hasil penelitian menunjukkan bahwa sistem mampu melakukan pembacaan *security alert*, analisis alamat IP, penyimpanan hasil ke MongoDB, serta penyajian hasil melalui *dashboard* dan laporan PDF. Rata-rata *Overall Latency* sebesar 252,42 ms, VirusTotal API *Latency* sebesar 250,53 ms, dan *Internal Processing Latency* sebesar 1,89 ms. Hasil tersebut menunjukkan bahwa sistem mampu mendukung proses *Threat Hunting* secara otomatis dengan waktu pemrosesan internal yang relatif kecil.

Kata kunci: *Threat Hunting*, Wazuh, VirusTotal, MongoDB, *Dashboard Monitoring*, Keamanan Siber.

UNIVERSITAS
GADJAH MADA
**Rancang Bangun Sistem Otomatisasi Threat Hunting Untuk Analisis Sumber Serangan Menggunakan Wazuh
dengan Intergrasi VirusTotal dan MongoDB**
Gagat Wijaya, Dr. Ir. Ronald Adrian, S.T., M.Eng., IPM., ASEAN Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

The increasing complexity of cyber threats requires the Threat Hunting process to be carried out quickly and efficiently. However, security alert analysis is still commonly performed manually, resulting in delays in identifying attack sources. This research aims to design and develop an automated Threat Hunting system for attack source analysis using Wazuh integrated with VirusTotal and MongoDB. The system was developed using Python with a modular architecture. Wazuh was utilized as the security alert source, VirusTotal for public IP reputation analysis, MongoDB for storing analysis results, and Streamlit for providing a real time monitoring dashboard and Reportlab for generating PDF reports. The system was evaluated using two testing scenarios: PCAP dataset replay obtained from Malware Traffic Analysis and a real time SSH Brute Force attack simulation from Kali Linux against an Ubuntu Desktop target. Performance testing was conducted through 30 latency measurements collected from two dataset replay sessions. The results show that the system successfully performs automated security alert processing, IP reputation analysis, data storage, and monitoring. The average Overall Latency was 252.42 ms, the average VirusTotal API Latency was 250.53 ms, and the average Internal Processing Latency was 1.89 ms. These results indicate that the proposed system can support automated Threat Hunting with low internal processing time.

Keywords: Threat Hunting, Wazuh, VirusTotal, MongoDB, Monitoring Dashboard, Cybersecurity.