

**PENGEMBANGAN SISTEM ACTIVE RESPONSE DAN NOTIFIKASI
REAL-TIME UNTUK DETEKSI MALWARE DI PT. WIKA BETON**

SKRIPSI

Diajukan untuk memenuhi Sebagian dari persyaratan dalam memperoleh gelar
Sarjana Teknik pada Program Studi Sistem Telekomunikasi



Oleh:

Surya Kusuma

2100308

**PROGRAM STUDI SISTEM TELEKOMUNIKASI
KAMPUS UPI DI PURWAKARTA
UNIVERSITAS PENDIDIKAN INDONESIA
2025**

***PENGEMBANGAN SISTEM ACTIVE RESPONSE DAN NOTIFIKASI
REAL-TIME UNTUK DETEKSI MALWARE DI PT. WIKA BETON***

Oleh

Surya Kusuma

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Teknik pada Program Studi Sistem Telekomunikasi

© **Surya Kusuma**

Universitas Pendidikan Indonesia

Juli 2025

Hak Cipta dilindungi oleh undang-undang
Skripsi ini tidak boleh diperbanyak seluruhnya atau Sebagian,
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

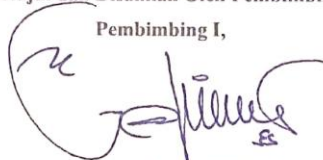
LEMBAR PENGESAHAN

Surya Kusuma
2100308

PENGEMBANGAN SISTEM ACTIVE RESPONSE DAN NOTIFIKASI
REAL-TIME UNTUK DETEKSI, MALWARE DI PT. WIKA BETON

Disetujui dan Disahkan Oleh Pembimbing:

Pembimbing I,



Galura Muhammad Suranegara, S.Pd., M.T.

NIP. 920190219920111101

Pembimbing II



Ichwan Nul Ichsan, S.T., M.T.

NIP. 920200119900330101

Mengetahui,

Ketua Program Studi Sistem Telekomunikasi



Galura Muhammad Suranegara, S.Pd., M.T.

NIP. 920190219920111101

ABSTRAK

Respon yang lambat dan manual terhadap ancaman siber menjadi tantangan signifikan bagi keamanan infrastruktur TI perusahaan. Sistem deteksi konvensional seringkali tidak memiliki kemampuan mitigasi otomatis, sehingga meningkatkan risiko kerusakan akibat *malware*. Penelitian ini bertujuan untuk mengembangkan dan menganalisis performa sistem *active response* otomatis berbasis Wazuh, yang diintegrasikan dengan VirusTotal API untuk akurasi deteksi dan notifikasi *real-time* Telegram untuk pelaporan instan. Penelitian ini menggunakan metode eksperimental pada tiga *agent* dengan sistem operasi berbeda (Ubuntu, Windows, CentOS) menggunakan *file* uji EICAR sebanyak 15 kali percobaan untuk setiap *agent*. Performa sistem diukur menggunakan metrik waktu respon, tingkat akurasi deteksi, dan kecepatan notifikasi. Hasil penelitian menunjukkan sistem mencapai tingkat akurasi deteksi 100% di semua platform. Waktu respon keseluruhan menunjukkan kinerja yang sangat cepat pada lingkungan Linux (rata-rata 2,010 detik pada CentOS dan 2,118 detik pada Ubuntu), namun lebih lambat pada Windows (rata-rata 12,519 detik) yang utamanya dipengaruhi oleh beban kerja pemindaian *File Integrity Monitoring* (FIM) pada direktori dengan banyak *file*. Untuk notifikasi Telegram berhasil terkirim dalam 1-2 detik setelah mitigasi. Kesimpulannya, sistem yang dikembangkan terbukti menjadi solusi yang efektif, cepat, dan akurat untuk otomatisasi deteksi dan respons *malware*, sekaligus menyoroti pentingnya pengaruh lingkungan sistem operasi terhadap performa *active response*.

Kata Kunci: *Wazuh, Active Response, VirusTotal, Deteksi Malware, Keamanan Siber*

ABSTRACT

Slow and manual responses to cyber threats pose a significant challenge to corporate IT infrastructure security. Conventional detection systems often lack automated mitigation capabilities, increasing the risk of damage from malware. This research aims to develop and analyze the performance of an automated active response system based on Wazuh, integrated with the VirusTotal API for detection accuracy and real-time Telegram notifications for instant reporting. This study uses an experimental method on three agents with different operating systems (Ubuntu, Windows, CentOS), using the EICAR test file for 15 trials per agent. System performance was measured using metrics of response time, detection accuracy rate, and notification speed. The results show that the system achieved a 100% detection accuracy rate across all platforms. The overall response time demonstrated very fast performance in Linux environments (an average of 2.010 seconds on CentOS and 2.118 seconds on Ubuntu), but was slower on Windows (an average of 12.519 seconds), primarily influenced by the workload of File Integrity Monitoring (FIM) scans on directories with a large number of files. Telegram notifications were successfully delivered within 1-2 seconds post-mitigation. In conclusion, the developed system is proven to be an effective, fast, and accurate solution for automated malware detection and response, while also highlighting the significant influence of the operating system's environment on active response performance.

Keywords: Wazuh, Active Response, VirusTotal, Malware Detection, Cyber Security.

DAFTAR ISI

ABSTRAK	iii
<i>ABSTRACT</i>	iv
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	viii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Manfaat Penelitian	3
1.4.1 Secara Teoritis	3
1.4.2 Secara Praktis	3
1.5 Ruang Lingkup Penelitian	3
BAB II KAJIAN PUSTAKA	5
2.1 Keamanan Siber dan Ancaman <i>Malware</i>	5
2.2 Wazuh	6
2.3 VirusTotal	7
2.4 <i>Active Response</i>	8
2.5 Bot Telegram	9
2.6 Penelitian Terdahulu	10
BAB III METODE PENELITIAN	11
3.1 Alur Penelitian	11
3.1.1 Studi Literatur	12

3.1.2	Persiapan Sistem	12
3.1.3	Desain Sistem.....	12
3.1.4	Pengujian Sistem.....	16
3.1.5	Analisis Data	17
3.2	Spesifikasi Perangkat Penelitian	18
BAB IV HASIL DAN PEMBAHASAN		21
4.1	Hasil dan Pembahasan Pengembangan Sistem	21
4.2	Hasil dan Pembahasan Skenario Pengujian <i>Malware</i>	23
4.2.1	Pengukuran I	24
4.2.2	Pengukuran II	26
4.2.3	Pengukuran III.....	28
4.3	Hasil dan Pembahasan Pengujian.....	30
4.3.1	Hasil dan Pembahasan Pengukuran I, II, dan III.....	31
4.3.2	Hasil dan Pembahasan Kinerja Keseluruhan Sistem	33
BAB V SIMPULAN DAN SARAN		38
5.1	Kesimpulan	38
5.2	Saran.....	39
DAFTAR PUSTAKA		40
LAMPIRAN.....		44

DAFTAR GAMBAR

Gambar 3. 1 Alur Penelitian.....	11
Gambar 3. 2 Desain Wazuh dan VirusTotal API.....	14
Gambar 3. 3 Desain Wazuh dan Telegram Bot.....	16
Gambar 3. 4 Pengujian Sistem	17
Gambar 4. 1 Integrasi VirusTotal API	22
Gambar 4. 2 Notifikasi <i>Real-time</i> Telegram	23
Gambar 4. 3 Grafik Perbandingan <i>Active Response Detection</i>	36

DAFTAR TABEL

Tabel 3. 1 Informasi <i>Hardware</i>	19
Tabel 3. 2 Informasi <i>Software</i>	20
Tabel 4. 1 Nilai rata-rata Pengukuran I.....	24
Tabel 4. 2 Nilai rata-rata Pengukuran II.....	27
Tabel 4. 3 Nilai rata-rata Pengukuran III	29
Tabel 4. 4 Hasil rata-rata Pengukuran I, II, dan III	32
Tabel 4. 5 Nilai rata-rata Pengukuran kinerja sistem.....	33
Tabel 4. 6 Tabel Akurasi Sistem	35

DAFTAR PUSTAKA

- Aditya, Yusuf Muhyidin, & Dayan Singasatia. (2024). Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh. *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika*, 2(5), 137–144. <https://doi.org/10.61132/merkurius.v2i5.289>
- Farrel, F. I. F., Is Mardianto, S.Si, M.Kom, & Ir. Adrian Sjamsul Qamar, Mti. (2024a). Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System. *Intelmatiks*, 4(1), 1–7. <https://doi.org/10.25105/itm.v4i1.18529>
- Farrel, F. I. F., Is Mardianto, S.Si, M.Kom, & Ir. Adrian Sjamsul Qamar, Mti. (2024b). Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System. *Intelmatiks*, 4(1), 1–7. <https://doi.org/10.25105/itm.v4i1.18529>
- Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1), 1–7. <https://doi.org/10.30630/jitsi.3.1.59>
- Ghelani, D. (2022). *Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review*. Preprints. <https://doi.org/10.22541/au.166385207.73483369/v1>

- Harley, D., Myers, L., & Willems, E. (2011). Test Files and Product Evaluation: The Case for and against Malware Simulation. *AVAR (Association of Anti Virus Asia Researchers 13th Conference)*.
- Islam, M. R., & Rafique, R. (2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. *International Journal of Engineering Materials and Manufacture*, 9(4), 136–144. <https://doi.org/10.26776/ijemm.09.04.2024.02>
- Kantola, T. (2022). Exploring VirusTotal for security operations alert triage automation. *Information and Communication Technologies. Bachelor's Degree Programme in Information and Communications Technology*.
- Kumar, R. (2024). The Future of Cyber Threat Intelligence: Anticipating and Preparing for Evolving Threats. *International Journal of Innovative Science and Research Technology (IJISRT)*, 699–704. <https://doi.org/10.38124/ijisrt/ijisrt24sep430>
- Nurhayati, A. (2020). MONITORING SISTEM KEAMANAN JARINGAN BERBASIS TELEGRAM BOT PADA LOCAL AREA NETWORK. *Journal of Informatics and Communication Technology (JICT)*, 1(2), 45–53. https://doi.org/10.52661/j_ict.v1i2.41
- Patil, C. (2024). Real Time Threat Intelligence System for Malware Detection. *International Journal for Research in Applied Science and Engineering Technology*, 12(4), 5204–5208. <https://doi.org/10.22214/ijraset.2024.61086>
- Peng, P., Yang, L., Song, L., & Wang, G. (2019). Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines. *Proceedings of the*

Internet Measurement Conference, 478–485.

<https://doi.org/10.1145/3355369.3355585>

Salem, A., Banescu, S., & Pretschner, A. (2020). *Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection* (No. arXiv:2007.00510). arXiv. <https://doi.org/10.48550/arXiv.2007.00510>

Shafiyah, A., Nama, G. F., & Pradipta, R. A. (2024). IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER. *Jurnal Informatika dan Teknik Elektro Terapan*, 12(2). <https://doi.org/10.23960/jitet.v12i2.4074>

Shelke, R. R. (2024). Active Security Surveillance and Object Detection. *International Journal of Information Technology & Computer Engineering*, 4(5), 38–47. <https://doi.org/10.55529/ijitc.45.38.47>

Sholeh, M., & Monalisa, A. (2024). MEMBANGUN AGENT ENDPOINT DETECTION AND RESPONSE (EDR) MENGGUNAKAN WAZUH DAN VIRUSTOTAL SEBAGAI SISTEM DETEKSI SERANGAN RANSOMWARE LOCKBIT 3.0. *Infotech: Journal of Technology Information*, 10(2), 279–288. <https://doi.org/10.37365/jti.v10i2.320>

Stanković, S., Gajin, S., & Petrović, R. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. *IX INTERNATIONAL CONFERENCE IcETRAN*.

- Uhm, W. P. (2022). Real-Time Network Intrusion Prevention System Using Incremental Feature Generation. *Computers, Materials & Continua*, 70(1), 1631–1648. <https://doi.org/10.32604/cmc.2022.019667>
- Widyantono, D. P., & Sulisty, W. (2023). Pemodelan InstrusionPreventionSystemUntuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan Wazuh. *Journal of Information Technology Ampera*, 4(1).
- Zhao, K., Gong, S., & Fonseca, P. (2021). On-demand-fork: A microsecond fork for memory-intensive and latency-sensitive applications. *Proceedings of the Sixteenth European Conference on Computer Systems*, 540–555. <https://doi.org/10.1145/3447786.3456258>