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/

DAFTAR PUSTAKA

[1] B. S. Pamungkas and I. Sembiring, "ANALISIS SERANGAN CYBER MENGGUNAKAN HONEYPOT PADA WEB BERBASIS CLOUD," *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, vol. 4, no. 3, pp. 1284–1295, Sep. 2023, doi: 10.35870/jimik.v4i3.325.

[2] R. Aditya, "Implementasi *Security Information And Event Management* (SIEM) Untuk *Monitoring* Keamanan Server Menggunakan Wazuh."

[3] R. Aditya, "Implementasi *Security Information And Event Management* (SIEM) Untuk *Monitoring* Keamanan Server Menggunakan Wazuh."

[4] M. R. T. Hidayat, N. Widiyasono, and R. Gunawan, "OPTIMASI DETEKSI MALWARE PADA SIEM WAZUH MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, Jan. 2025, doi: 10.23960/jitet.v13i1.5686.

[5] N. Hidayasari, Mansur, Kasmawi, and Z. Efendi, "Implementasi Prototipe SIEM Berbasis Wazuh pada Website dengan Pengujian FIM dan *Threat Hunting*," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 4, pp. 372–382, Dec. 2025, doi: 10.62527/jitsi.6.4.523.

[6] M. A. Ekawan Putra, K. Marzuki, and I. P. Hariyadi, "OTOMATISASI KONFIGURASI WAZUH TERINTEGRASI VIRUSTOTAL MENGGUNAKAN ANSIBLE UNTUK MENDETEKSI DAN MEMPROTEKSI SERANGAN MALWARE," Jan. 2025.

[7] F. A. Saputra *et al.*, "Jurnal Informatika Terpadu IMPLEMENTASI WAZUH SIEM UNTUK MANAJEMEN LOG *EVEN*T DI PESANTREN TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG," *Jurnal Informatika Terpadu*, vol. 10, no. 2, pp. 146–155, 2024, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[8] B. Haryanto and D. W. Chandra, "Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW," *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, vol. 5, no. 1, pp. 183–192, Jan. 2024, doi: 10.35870/jimik.v5i1.447.

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/

[9] E. Wardani, "KEAMANAN INFORMASI PERPUSTAKAAN PUBLIK: STUDI KASUS DAN PENDEKATAN CIA TRIAD," *JIPKA*, vol. 5, no. 1, p. 2025, doi: 10.26418/ji.

[10] T. Rochmadi and I. Y. Pasa, "MEASUREMENT OF RISK AND EVALUATION OF INFORMATION *SECURITY* USING THE INFORMATION *SECURITY* INDEX IN BKD XYZ BASED ON ISO 27001 / SNI," 2021.

[11] A. H. Harahap, C. Difa Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder".

[12] R. D. Anggaini Puspita, P. Dahlian Persadha, and S. Tinggi Intelijen Negara, "Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi Vital Terhadap Stabilitas Keamanan Nasional," *Syntax Literate*, vol. 10, no. 5, 2025.

[13] E. Syah, H. Weharima, T. Susilo, T. Basuki, and A. M. Akad, "Serangan Siber terhadap Infrastruktur Kritis," *JURNAL SYNTAX IMPERATIF : Jurnal Ilmu Sosial dan Pendidikan*, vol. 6, no. 2, pp. 145–154, May 2025, doi: 10.54543/syntaximperatif.v6i2.678.

[14] R. Baltwin Tallane and D. W. Chandra, "IMPLEMENTATION OF INTRUSION DETECTION SYSTEM (IDS) USING *SECURITY* ONION," vol. 7, no. 10, 2022.

[15] A. Kristian, R. Skavinsky Teddy, V. P. Meylani, and D. P. Kesuma, "Strategi Mitigasi Ancaman Siber di Era Teknologi Berkembang: Systematic Literature Review," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 8, no. 3, 2025.

[16] F. Nursyahiddin, S. Zulfa Oktaviani, L. Dwi Iklima, and F. Nurdiyanti, "PENGENALAN AKTIFITAS CYBER *THREAT HUNTING* : STUDI KASUS HUNTING MALWARE DENGAN METODE MEMORY FORENSIC," *Journal of Computer Science and Technology (JCS-TECH)*, vol. 2, no. 1, pp. 8–13, May 2022, doi: 10.54840/jcstech.v2i1.20.

[17] N. Hidayasari, Mansur, Kasmawi, and Z. Efendi, "Implementasi Prototipe SIEM Berbasis Wazuh pada Website dengan Pengujian FIM dan *Threat Hunting*," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 4, pp. 372–382, Dec. 2025, doi: 10.62527/jitsi.6.4.523.

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/

[18] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, “Guide to Cyber Threat Information Sharing,” Gaithersburg, MD, Oct. 2016. doi: 10.6028/NIST.SP.800-150.

[19] M. A. Ekawan Putra, I. P. Hariyadi, and K. Marzuki, “OTOMATISASI KONFIGURASI WAZUH TERINTEGRASI VIRUSTOTAL MENGGUNAKAN ANSIBLE UNTUK MENDETEKSI DAN MEMPROTEKSI SERANGAN MALWARE,” Jan. 2025.

[20] H. Ghianni, M. Zhang, J. P. Galeotti, and A. Arcuri, “Search-Based Fuzzing For RESTful APIs That Use MongoDB,” Jul. 2025, [Online]. Available: http://arxiv.org/abs/2507.20848