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 ISI

SAMPUL LAPORAN PROYEK AKHIR 1
LEMBAR PENGESAHAN i
PERNYATAAN BEBAS PLAGIASI ii
KATA PENGANTAR iii
DAFTAR ISI vi
DAFTAR GAMBAR x
DAFTAR TABEL xii
INTISARI xiii
ABSTRACT xiv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 3
1.4 Batasan Masalah 3
1.5 Manfaat Penelitian 4
1.6 Sistematika Penelitian 4
BAB II TINJAUAN PUSTAKA 6
2.1 Tinjauan Pustaka 6
2.2 Dasar Teori 12
2.2.1 Keamanan Informasi 12
2.2.2 Ancaman, Kerentanan dan Serangan 13
2.2.3 Threat Hunting 14
2.2.4 *Security Information and Event Management* (SIEM) 15
2.2.5 Threat Intelligence 16

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/

2.2.6 Wazuh 17
2.2.7 VirusTotal 17
2.2.8 MongoDB 18
2.2.9 Python 18
2.2.10 *Aplication Proramming Interface* (API) 18
2.2.11 Kali Linux 19
2.2.12 Ubuntu 19
2.2.13 Hipotesis 19
BAB III METODE PENELITIAN 21
3.1 Peralatan Penelitian 21
3.1.1 Perangkat Keras 21
3.1.2 Perangkat Lunak 21
3.2 Tahapan Penelitian 25
3.3 Perancangan Sistem 30
3.3.1 Arsitektur Sistem Proyek 30
3.3.2 Perancangan Sistem Otomatisasi *Threat Hunting* 31
3.3.3 Perancangan Modul Sistem Otomatisasi 34
3.3.4 Perancangan Basis Data MongoDB 37
3.3.5 Perancangan *Dashboard Monitoring* 40
3.3.6 Perancangan *Threat Hunting Report* 42
BAB IV HASIL DAN PEMBAHASAN 45
4.1 Implementasi Lingkungan Penelitian 45
4.1.1 Implementasi Perangkat Keras 47
4.1.2 Implementasi Perangkat Lunak 48
4.2 Implementasi Sistem 53
4.2.1 Implementasi Wazuh 53

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/

4.2.2 Implementasi MongoDB 56
4.2.3 Implementasi Sistem Otomatisasi *Threat Hunting* 61
4.2.4 Implementasi *Dashboard Monitoring* 64
4.2.5 Implementasi Pembuatan Laporan PDF 72
4.2.6 Implementasi *Threat Hunting Report* 74
4.3 Pengujian Sistem 81
4.3.1 Pengujian *Parser* PCAP 81
4.3.2 Pengujian Serangan Langsung 84
4.3.3 Pengujian Integrasi Wazuh 87
4.3.4 Pengujian Sistem Otomatisasi *Threat Hunting* 88
4.3.5 Pengujian MongoDB 91
4.3.6 Pengujian *Dashboard Monitoring* 92
4.3.7 Pengujian *Threat Hunting Report* 96
4.3.8 Pengujian Performa Sistem *Threat Hunting (Latency)* 97
4.4 Analisis Hasil Pengujian 100
4.4.1 Analisis Pengujian Parser PCAP 100
4.4.2 Analisis Pengujian Serangan Langsung 101
4.4.3 Analisis Pengujian Integrasi Wazuh 101
4.4.4 Analisis Pengujian Sistem Otomatisasi *Threat Hunting* 101
4.4.5 Analisis Pengujian MongoDB 101
4.4.6 Analisis Pengujian *Dashboard Monitoring* 102
4.4.7 Analisis Pengujian *Threat Hunting Report* 102
4.4.8 Analisis Pengujian Performa Sistem (Latensi) 102
4.4.9 Analisis Keseluruhan Sistem 103
BAB V PENUTUP 104
5.1 Kesimpulan 104

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/

5.2 Saran 104

DAFTAR PUSTAKA 106

LAMPIRAN 109