



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**RANCANG BANGUN SISTEM OTOMASI PADA
WAZUH MENGGUNAKAN VALIDASI MULTI-
SOURCE CTI UNTUK MITIGASI *MALWARE***

Sub-judul

**ANALISIS KINERJA OTOMATISASI PADA WAZUH
DAN SURICATA UNTUK MITIGASI *MALWARE***

SKRIPSI

BAYU DWI SETIANTO 2207421008

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER**

POLITEKNIK NEGERI JAKARTA

2026



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



ANALISIS KINERJA OTOMATISASI PADA WAZUH DAN SURICATA UNTUK MITIGASI *MALWARE*

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk
Memperoleh Diploma Empat Politeknik**

BAYU DWI SETIANTO

2207421008

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Bayu Dwi Setianto
NIM : 2207421008
Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul skripsi : ANALISIS KINERJA OTOMATISASI PADA WAZUH DAN SURICATA UNTUK MITIGASI *MALWARE*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya seni orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 9 Juni 2026

yang membuat pernyataan



Bayu Dwi Setianto

NIM 2207421008



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Bayu Dwi Setianto
NIM : 2207421008
Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul skripsi : Analisis Kinerja Otomatisasi Pada Wazuh Dan Suricata Untuk Mitigasi *Malware*
Telah diuji oleh tim penguji dalam sidang skripsi pada hari *Rabu*.... Tanggal *17*..., Bulan *Juni*..., Tahun *2016* dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Asep Kurniawan, S.Pd., M.Kom ()
Penguji I : Ayu Rosyida Zain, S.ST, M.T. ()
Penguji II : Dr. Defiana Arnaldi, S.T.P., M.Si. ()
Penguji III : Andika Riyadi Jasril, M.Pd.T. ()

Mengetahui :
Jurusan Teknik Informatika dan Komputer
Ketua


Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji syukur senantiasa penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga skripsi yang berjudul "Analisis Kinerja Otomatisasi pada Wazuh dan Suricata untuk Mitigasi *Malware*" ini dapat diselesaikan dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Diploma Empat Politeknik. Penulis menyadari bahwa penyelesaian skripsi ini tidak lepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Asep Kurniawan, S.Pd., M.Kom., selaku dosen pembimbing atas kesabaran, waktu, serta arahan teknisnya yang sangat berharga selama proses penelitian dan penyusunan skripsi ini.
2. Kedua orang tua dan keluarga besar, atas doa yang tak pernah putus, serta dukungan moral maupun material yang selalu menyertai langkah penulis dari awal perkuliahan hingga saat ini.
3. Muhammad Ilham Utama, selaku rekan penelitian yang telah berjuang bersama. Terima kasih juga kepada Raden Muhammad Fadil Azhar, Stephanie Meissya Permata Asri Tarigan, dan Harsdyka Wibisono selaku sahabat-sahabat terbaik, serta seluruh rekan Program Studi Teknik Multimedia dan Jaringan angkatan 2022 atas diskusi dan kebersamaan yang berkesan.
4. Beauty Fatimah Rahayu, atas pengertian, doa, serta dukungan emosional luar biasa yang senantiasa menyemangati penulis di setiap tantangan pengerjaan skripsi ini.

Penulis menyadari sepenuhnya bahwa skripsi ini masih memiliki kekurangan akibat keterbatasan pengalaman dan pengetahuan. Oleh karena itu, kritik serta saran yang membangun sangat penulis harapkan. Akhir kata, semoga skripsi ini bermanfaat, menambah wawasan akademis, dan memberikan kontribusi positif bagi perkembangan teknologi keamanan siber.

Depok, Juni 2026
Bayu Dwi Setianto



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini :

Nama : Bayu Dwi Setianto
NIM : 2207421008
Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik
Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Analisis Kinerja Otomatisasi Pada Wazuh Dan Suricata Untuk Mitigasi *Malware*.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 08 Juni 2026
Yang membuat pernyataan,



Bayu Dwi Setianto
NIM. 2207421008



ANALISIS KINERJA OTOMATISASI PADA WAZUH DAN SURICATA UNTUK MITIGASI *MALWARE*

ABSTRAK

Serangan siber berupa penyebaran malware dan eksploitasi jaringan semakin masif serta membutuhkan waktu respons yang sangat cepat. Penanganan insiden keamanan secara manual sering menimbulkan latency yang berpotensi memperburuk dampak serangan siber. Penelitian ini bertujuan menganalisis kinerja otomatisasi pada Wazuh dan Suricata untuk mitigasi malware. Pendekatan eksperimental digunakan melalui integrasi Wazuh sebagai Security Information and Event Management (SIEM), Suricata sebagai Network Intrusion Detection System (NIDS), dan router MikroTik sebagai gateway. Sampel uji menggunakan Indicator of Compromise (IoC) yang telah divalidasi malicious oleh sistem Multi-CTI eksternal. Hal ini menegaskan bahwa fokus penelitian murni pada kecepatan eksekusi Active Response, bukan pada analisis klasifikasi malware itu sendiri. Pengujian membandingkan waktu respons manual dengan mitigasi otomatis, yang meliputi penghapusan file di endpoint dan pemblokiran IP sumber. Hasil pengujian membuktikan sistem berhasil mengeksekusi pertahanan secara otomatis. Sistem mampu memangkas rata-rata waktu respons dari 148,8 detik (manual) menjadi 3,102 detik (otomatis). Implementasi ini menghasilkan tingkat efisiensi mitigasi sebesar 97,91% dengan percepatan mencapai 47,97 kali lipat. Kesimpulannya, otomatisasi pada Wazuh dan Suricata sangat efektif mempercepat respons mitigasi dan meminimalisasi celah keamanan pada infrastruktur jaringan.

Kata Kunci: Otomasi, Wazuh, SIEM, Suricata, Mitigasi Otomatis, Malware.

POLITEKNIK
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME	iii
LEMBAR PENGESAHAN	iv
KATA PENGANTAR	v
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	vi
ABSTRAK	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Perumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan dan Manfaat	3
1.5. Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1 Penelitian Terdahulu	6
2.2 Landasan Teori	8
2.2.1 <i>Security Orchestration, Automation, and Response (SOAR)</i>	8
2.2.2 <i>Security Information and Event Management (SIEM)</i>	8
2.2.3 Wazuh	8
2.2.4 <i>Server</i>	9
2.2.5 <i>Network Intrusion Detection System</i>	9
2.2.6 <i>File integrity monitoring (FIM)</i>	10
2.2.7 <i>Active Response</i>	10
2.2.8 Suricata	11
2.2.9 <i>Extended Detection and Response (XDR)</i>	12
2.2.10 Flowchart	12
2.2.11 Mikrotik	12
2.2.12 <i>Malware</i>	13
2.2.13 <i>Firewall</i>	13
2.2.14 Python	14
2.2.15 PolarProxy	14



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.2.16	Router.....	14
2.2.17	<i>Speedup Test</i>	15
2.2.18	<i>Security Operation Center</i>	15
2.2.19	<i>Incident Response Lifecycle</i>	16
2.2.20	<i>Cyber Threat Intelligence (CTI)</i>	16
2.2.21	<i>Indicator of Compromise (IoC)</i>	16
2.2.22	<i>TLS/SSL Inspection</i>	17
2.2.23	<i>Application Programming Interface (API)</i>	17
2.2.24	<i>Asynchronous Processing</i>	17
BAB III METODE PENELITIAN.....		19
3.1	Rancangan Penelitian.....	19
3.1.1	Metode Penelitian.....	19
3.1.2	Teknik Pengumpulan Data dan Analisis.....	19
3.2	Tahapan Penelitian.....	20
3.3	Objek Penelitian.....	23
BAB IV HASIL DAN PEMBAHASAN.....		24
4.1	Analisis Kebutuhan.....	24
4.1.1	Spesifikasi Sistem	24
4.1.2	Konfigurasi Jaringan.....	24
4.2	Perancangan Sistem	25
4.2.1	Topologi Sistem	25
4.2.2	Diagram Blok Sistem.....	27
4.2.3	Arsitektur <i>TLS Inspection</i>	28
4.2.4	Flowchart Sistem.....	29
4.2.4.1	Flowchart Penghapusan <i>File</i>	30
4.2.4.2	Flowchart <i>Block IP</i>	31
4.3	Implementasi Sistem.....	32
4.3.1	Persiapan Lingkungan Virtual.....	32
4.3.2	Implementasi Pedeteksian <i>Alert</i>	43
4.3.3	Implementasi Pembuatan Log <i>Active Response</i>	45
4.3.4	Implementasi <i>Active Response</i>	49
4.3.5	Implementasi Mitigasi.....	52
4.4	Pengujian Sistem.....	54
4.4.1	Deskripsi Pengujian Sistem.....	54
4.4.2	Prosedur Pengujian	55
4.4.3	Sampel Data Uji	56



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.4 Data Hasil Pengujian.....	58
BAB V PENUTUP.....	62
5.1 Kesimpulan	62
5.2 Saran.....	62
DAFTAR PUSTAKA	64
DAFTAR RIWAYAT HIDUP.....	68
LAMPIRAN.....	69





DAFTAR GAMBAR

Gambar 2. 1 Logo Wazuh	9
Gambar 2. 2 Contoh Inline Network-Based IDPS Sensor Architecture	10
Gambar 2. 3 Definisi FIM	10
Gambar 2. 4 Diagram alur Active Response	11
Gambar 2. 5 Logo Suricata	11
Gambar 2. 6 Contoh Flowchart	12
Gambar 2. 7 Logo PolarProxy	14
Gambar 3. 1 Alur Penelitian	20
Gambar 3. 2 Ruang Lingkup Penelitian Kinerja Sistem	22
Gambar 4. 1 Topologi Sistem	25
Gambar 4. 2 Diagram Blok Sistem	27
Gambar 4. 3 Arsitektur TLS Inspection	28
Gambar 4. 4 Flowchart penghapusan File	30
Gambar 4. 5 Flowchart Block IP	31
Gambar 4. 6 Wazuh OVA	33
Gambar 4. 7 Wazuh Adapter	33
Gambar 4. 8 Wazuh Dashboard	34
Gambar 4. 20 Instalasi PolarProxy	35
Gambar 4. 21 Pembuatan Sertifikasi PolarProxy	35
Gambar 4. 22 Pre-Filtered Log	36
Gambar 4. 23 Install Wazuh Agent di Suricata Server	36
Gambar 4. 24 Penambahan file Monitor di Suricata	37
Gambar 4. 11 Install Wazuh Agent di Endpoint	37
Gambar 4. 25 Download Sertifikat dari Suricata Server	38
Gambar 4. 26 Konversi cer ke crt	38
Gambar 4. 27 Install Sertifikat di Endpoint	38
Gambar 4. 13 IP Lokal Mikrotik	39
Gambar 4. 14 DHCP Pool	39
Gambar 4. 15 IP Reservation	40
Gambar 4. 16 Penanda Protokol	40
Gambar 4. 17 Perutean Jaringan	41
Gambar 4. 18 API Port Mikrotik	41
Gambar 4. 19 Filter Rules Mikrotik	42
Gambar 4. 12 FIM Endpoint	43
Gambar 4. 9 Suricata Home-Net	44
Gambar 4. 10 Suricata Output-Set	44
Gambar 4. 33 Fungsi pembacaan alert FIM	46
Gambar 4. 34 Fungsi pembacaan alert FIM	46
Gambar 4. 35 Response mitigasi Malicious Files	47
Gambar 4. 36 Fungsi Penambahan Blacklist Hash ke CDB List	47
Gambar 4. 37 Fungsi Pembuatan log ke Chimera SOAR	47
Gambar 4. 38 Fungsi Cek Kesamaan Hash di CDB List	48
Gambar 4. 39 Fungsi Mitigasi jika ada kesamaan dengan CDB List	48
Gambar 4. 40 Fungsi utama Monitor Suricata	49
Gambar 4. 28 Konfigurasi Active Response Remove-Threat	49
Gambar 4. 29 Aturan Chimera SOAR Block IP	50

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4. 30 Pemantauan Log Chimera SOAR	50
Gambar 4. 31 Pemantauan Log Chimera CTI.....	51
Gambar 4. 32 Pemantauan Log Chimera IP.....	51
Gambar 4. 41 Script Remove-threat.....	53
Gambar 4. 42 Script Block-Mikrotik	53





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	6
Tabel 4. 1 Spesifikasi Sistem	24
Tabel 4. 2 Rancangan Jaringan	25
Tabel 4. 3 Ringkasan Kostumisasi Rules	51
Tabel 4. 4 Sampel Pengujian Sistem	56
Tabel 4. 5 Hasil Pengujian Fungsionalitas Sistem	59
Tabel 4. 6 Hasil Pengujian Waktu Respons Mitigasi Manual	60
Tabel 4. 7 Hasil Pengujian Waktu Respons Mitigasi Otomatis	61



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1. Latar Belakang

Dalam era transformasi digital saat ini, vektor serangan siber telah berkembang menjadi sangat kompleks (Susanto *et al.*, 2023). Serangan siber modern jarang beroperasi melalui satu jalur tunggal, melainkan sering kali mengkombinasikan penyusupan *malware* pada tingkat *endpoint* dengan aktivitas tersembunyi melalui jaringan. Fenomena ini menciptakan tantangan ganda bagi administrator keamanan, yakni keharusan untuk mendeteksi *file* berbahaya yang berhasil menyusup, sekaligus secara bersamaan mencegah aktivitas pengunduhan *malware* tambahan dari sumber atau *server* eksternal yang teridentifikasi mendistribusikan *malware* tersebut.

Namun demikian, kondisi di lapangan menunjukkan bahwa banyak organisasi masih mempertahankan arsitektur keamanan yang terfragmentasi. Sistem pertahanan di sisi *endpoint* dan di sisi jaringan sering kali bekerja secara terisolasi tanpa adanya pertukaran informasi. Celah dari ketidaksinkronan ini sangat rentan dieksploitasi oleh penyerang untuk memperluas area infeksi di dalam infrastruktur target (Indah Novitasari, 2017).

Metode mitigasi manual yang selama ini diterapkan justru memperburuk kerentanan sistem. Ketika penanganan ancaman bergantung pada intervensi manusia, proses analisis log dan konfigurasi pemblokiran tidak dapat dilakukan secara seketika. Selama intervensi manual belum dieksekusi, jalur komunikasi menuju *server* yang mendistribusikan *malware* tetap dibiarkan aktif. Jeda waktu penanganan ini sangat berisiko karena memberikan kesempatan bagi sistem yang terkompromi untuk menyelesaikan proses pengunduhan *malware* berbahaya. Oleh karena itu, terdapat urgensi yang sangat tinggi untuk segera memblokir alamat IP dari sumber distributor *malware* secepat mungkin, guna memutus koneksi dan menghentikan proses pengunduhan sebelum infeksi menyebar lebih luas ke perangkat lain.

Untuk menjawab tantangan tersebut, diperlukan sebuah mekanisme mitigasi



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

otomatis terpadu yang menyinkronkan deteksi ancaman pada tingkat jaringan dan *endpoint* secara *real-time*. Dalam penelitian ini, Suricata diandalkan sebagai *Network Intrusion Detection System* yang secara spesifik bertugas untuk mendeteksi keberadaan *malware* yang melintas pada *traffic* jaringan. Sementara itu, Wazuh dipilih karena memiliki kapabilitas *Endpoint Detection and Response* yang tangguh untuk mendeteksi anomali *file* langsung di perangkat target. Kombinasi kedua instrumen open-source ini diintegrasikan ke dalam sebuah subsistem *Security Orchestration, Automation, and Response* yang berkolaborasi dengan modul *Cyber Threat Intelligence* (CTI).

Berdasarkan hasil validasi CTI yang menyatakan status *file* tersebut berbahaya, sistem otomasi secara otomatis akan mengeksekusi tindakan mitigasi ganda dalam hitungan milidetik. Tindakan pertama adalah menambahkan alamat IP server distributor *malware* ke dalam daftar blokir pada router MikroTik melalui *Application Programming Interface* untuk memutus koneksi pengunduhan muatan berbahaya secara instan pada lapisan jaringan. Tindakan kedua dilakukan secara simultan berupa penghapusan *file* berbahaya pada perangkat *endpoint* untuk melakukan sterilisasi sistem lokal. Penelitian ini berfokus pada analisis efektivitas kinerja otomatisasi tersebut dalam mempercepat waktu respons dan menutup celah kerentanan infrastruktur secara komprehensif.

1.2. Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang Sistem Otomatisasi Pada Wazuh Dan Suricata Untuk Mitigasi *Malware*?
2. Bagaimana efektivitas sistem otomatisasi tersebut dalam menurunkan waktu respons mitigasi dibandingkan dengan metode penanganan manual?

1.3. Batasan Masalah

Fokus penelitian ini adalah sebagai berikut :



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1. Fokus pada mekanisme Eksekusi Mitigasi otomatis dan integrasi perangkat (Wazuh-Suricata-MikroTik).
2. Mitigasi menggunakan *Script* Python untuk injeksi *Block List* IP dan Penghapusan *file* pada OS Linux.
3. Validasi ancaman dilakukan oleh sistem mitra, penelitian ini hanya menerima output keputusan *Malicious* atau *Safe*.
4. Sampel *file* berbahaya yang digunakan merupakan data IoC yang telah diklasifikasikan berstatus *malicious* oleh sistem Multi-CTI rekan penelitian.
5. Penelitian ini tidak melakukan analisis statis maupun dinamis terhadap struktur, perilaku, atau varian *malware* tersebut.
6. Objek analisis dalam penelitian ini adalah kinerja mekanisme *Active Response* berupa percepatan dan ketepatan eksekusi mitigasi *block IP* dan penghapusan *file* yang dipicu oleh keluaran log *chimera_soar.json* setelah *verdict malicious* diterima dari sistem mitra.

1.4. Tujuan dan Manfaat

Adapun tujuan dari penelitian ini antara lain :

1. Merancang Sistem Otomatisasi Pada Wazuh Dan Suricata Untuk Mitigasi *Malware*.
2. Menganalisis efektivitas kinerja Sistem Otomatisasi Pada Wazuh Dan Suricata Untuk Mitigasi *Malware*.

Beberapa manfaat yang diharapkan dari penelitian ini antara lain :

1. Peningkatan Efisiensi Monitoring dan Analisis Log, Sistem ini memberikan kemudahan bagi administrator jaringan dalam mengelola log yang sebelumnya tersebar di berbagai perangkat menjadi terpusat dalam satu dashboard
2. Mitigasi Risiko Human Error dan Kelelahan, Otomatisasi respons mengurangi beban kognitif administrator yang harus memantau ribuan log setiap hari.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.5. Sistematika Penulisan

Berikut sistematika penulisan ke dalam lima bab dengan rincian sebagai berikut:

A. BAB 1: PENDAHULUAN

Bab 1 berisi gambaran umum mengenai dasar penelitian yang dilakukan. Di dalamnya mencakup latar belakang masalah mengenai urgensi penanganan serangan siber otomatis, identifikasi dan rumusan masalah, batasan masalah agar penelitian tetap terarah, tujuan yang ingin dicapai, manfaat penelitian bagi aspek teoritis dan praktis, serta sistematika penulisan laporan.

B. BAB 2: TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bab 2 memaparkan teori-teori pendukung dan studi literatur yang relevan dengan topik penelitian. Bagian ini membahas konsep dasar Keamanan Jaringan, *Security Orchestration, Automation, and Response* (SOAR), karakteristik serangan siber, serta tinjauan teknis mengenai perangkat lunak dan perangkat keras yang digunakan, meliputi Wazuh SIEM, Suricata NIDS, Router MikroTik, dan mekanisme komunikasi melalui API menggunakan bahasa pemrograman Python.

C. BAB 3: METODE PENELITIAN

Bab 3 menjelaskan tahapan-tahapan yang dilakukan dalam pelaksanaan penelitian. Pembahasan meliputi kerangka kerja penelitian, analisis kebutuhan sistem, perancangan topologi jaringan, desain arsitektur integrasi sistem otomatisasi, perancangan skenario serangan untuk pengujian, serta metode pengambilan data untuk pengukuran parameter kinerja sistem seperti waktu respon dan akurasi mitigasi.

D. BAB 4: HASIL DAN PEMBAHASAN

Bab 4 merupakan inti dari penelitian yang memuat hasil implementasi sistem dan analisis data pengujian. Di dalamnya dipaparkan proses instalasi dan konfigurasi Wazuh serta Suricata, implementasi modul *Active Response* pada Wazuh *Agent* dan MikroTik API, serta hasil pengujian terhadap simulasi serangan jaringan. Fokus utama bab ini adalah analisis komparatif kinerja sistem sebelum dan sesudah penerapan sistem otomatisasi,



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

serta pembahasan mengenai efektivitas mekanisme mitigasi otomatis dalam menangani intrusi.

E. BAB 5: PENUTUP

Bab 5 berisi kesimpulan yang diambil berdasarkan hasil analisis dan pembahasan pada bab sebelumnya untuk menjawab rumusan masalah. Bab ini juga memuat saran-saran yang konstruktif untuk pengembangan penelitian selanjutnya agar sistem yang dibangun dapat disempurnakan di masa mendatang.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian arsitektur sistem otomasi yang telah dilakukan, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Arsitektur sistem otomasi yang diusulkan berhasil diimplementasikan dengan mengintegrasikan Wazuh, Suricata sebagai *Network IDS*, *Cyber Threat Intelligence* (CTI), serta router MikroTik secara sinkron. Sistem terbukti mampu menjalankan fungsionalitas deteksi *malware* secara *real-time*, memvalidasi status ancaman secara otomatis melalui CTI, dan mengeksekusi tindakan mitigasi *Active Response* berupa penghapusan *file malware* pada *endpoint* bersamaan dengan pemblokiran alamat IP sumber di jaringan. Selain itu, sistem terbukti memiliki kemampuan seleksi yang baik dalam mencegah *False Positive* pada file yang aman.
2. Implementasi sistem otomasi memberikan peningkatan efisiensi yang signifikan dalam penanganan insiden keamanan. Berdasarkan hasil pengujian komparatif, sistem otomatisasi ini mampu memangkas rata-rata total waktu respons dari 148,8 detik pada penanganan manual menjadi 3,102 detik. Hal ini menghasilkan percepatan atau *speedup* sebesar 47,97 kali lipat lebih cepat dibandingkan metode manual, dengan tingkat efisiensi waktu mitigasi mencapai 97,91%.

5.2 Saran

Meskipun sistem otomasi yang dikembangkan telah beroperasi sesuai dengan rancangan dan memberikan peningkatan kinerja yang signifikan, masih terdapat beberapa ruang lingkup yang dapat dikembangkan untuk penelitian selanjutnya:

1. Penelitian selanjutnya disarankan untuk menambah variasi respons otomatis yang tidak hanya terbatas pada penghapusan *file* dan pemblokiran IP. Tindakan mitigasi dapat diperluas mencakup karantina



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

endpoint dari jaringan lokal, penghentian paksa proses yang mencurigakan di sistem operasi, hingga pemulihan otomatis *file* yang terinfeksi.

2. Penambahan *interface* visual khusus untuk metrik otomasi akan sangat membantu administrator. *Dashboard* ini nantinya dapat menampilkan grafik analitik waktu nyata *real-time* mengenai total insiden yang dicegah, rata-rata latensi respons (SLA), dan peta sebaran IP penyerang secara visual.





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Al-Daej, S., & Al-Qurishi, M. (2023). *Security Information and Event Management (SIEM) with SOAR for Advanced Incident Response*. International Journal of Advanced Computer Science and Applications (IJACSA), 14(2).
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-61r2>
- Citraweb. (2020). MikroTik Academy: MTCNA Study Guide. Citraweb Solusi Teknologi.
- Eko Purwanto (2015) 'IMPLEMENTASI JARINGAN HOTSPOT DENGAN MENGGUNAKAN ROUTER MIKROTIK SEBAGAI PENUNJANG PEMBELAJARAN', *IMPLEMENTASI JARINGAN HOTSPOT DENGAN MENGGUNAKAN ROUTER MIKROTIK SEBAGAI PENUNJANG PEMBELAJARAN* [Preprint].
- Fielding, R. T. (2000). *Architectural Styles and the Design of Network-based Software Architectures* [Disertasi Doktorat, University of California, Irvine].
- Gartner. (2020). Market Guide for Security Orchestration, Automation and Response Solutions. Gartner Research.
- IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.
- Indah Novitasari (2017) 'BABAKBARUREJIMKEAMANANSIBER', *BABAK BARU REJIM KEAMANAN SIBER DI ASIA TENGGARA MENYOSONG ASEAN CONNECTIVITY 2025* [Preprint].
- Islam, C., Babar, M. A., & Nepal, S. (2019). A Multi-Vocal Review of Security Orchestration, Automation and Response (SOAR) Implementation. ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM).
- Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150).



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-150>

Jurnal, H. *et al.* (2024) 'JURNAL RISET TEKNIK KOMPUTER IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DALAM MENINGKATKAN KEAMANAN JARINGAN', *JURTIKOM*, 1(3). doi:10.69714/ee1r1q05.

Kent, K. and Souppaya, M. (no date) *Special Publication 800-92 Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology.*

Microsoft (2025) *XDR definition*, *Microsoft Security*. Available at: <https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr> (Accessed: 18 December 2025).

MikroTik. (2024). API Interface Documentation. MikroTik Wiki. Tersedia di: <https://help.mikrotik.com/docs/display/ROS/API>

Muhammad Ade Putra, I Putu Hariyadi, Khairan Marzuki. (2025). Otomatisasi Konfigurasi Wazuh Terintegrasi VirusTotal Menggunakan Ansible Untuk Mendeteksi dan Memproteksi Serangan *Malware*. Melek IT Information Technology Journal. <https://melekit-if.uwks.ac.id/melekit/article/download/403/228>

Nel, M. and Khiabani, H. (2021) *SAMHAIN: Host Based Intrusion Detection via File integrity monitoring* Martinus Nel *SAMHAIN: Host Based Intrusion Detection via File integrity monitoring GLAC (GSEC) Gold Certification SAMHAIN: Host Based Intrusion Detection via File integrity monitoring* | 2. Available at: <http://aide.sourceforge.net/>.

NIST. (2012). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). National Institute of Standards and Technology.

O'Connor, T. J. (2012). *Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers*. Syngress. (Opsional, tapi bagus untuk referensi Python di keamanan siber).



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

OISF (2025) *What is Suricata, Suricata Documentation*. Available at: <https://docs.suricata.io/en/latest/what-is-suricata.html> (Accessed: 16 December 2025).

Red Hat (2025) *System Auditing, Red Hat Documentation*. Available at: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/chap-system_auditing (Accessed: 16 December 2025).

Scarfone, K., & Hoffman, P. (2009). Guidelines on *Firewalls and Firewall Policy* (NIST Special Publication 800-41 Revision 1). National Institute of Standards and Technology.

Scarfone, K.A. and Mell, P.M. (2007) *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Gaithersburg, MD. doi:10.6028/NIST.SP.800-94.

Schryen, G. (2024). Speedup and efficiency of computational parallelization: A unifying approach and asymptotic analysis. *Journal of Parallel and Distributed Computing*, 187. <https://doi.org/10.1016/j.jpdc.2023.104835>

Sheffer, Y., Holz, R., & Saint-Andre, P. (2015). *Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)* (RFC 7457). Internet Engineering Task Force. <https://doi.org/10.17487/RFC7457>

SmartDraw (no date) *Flowchart Symbols, SmartDraw*. Available at: <https://www.smartdraw.com/flowchart/flowchart-symbols.htm> (Accessed: 18 December 2025).

Souppaya, M., & Scarfone, K. (2013). Guide to *Malware Incident Prevention and Handling for Desktops and Laptops* (NIST SP 800-83 Rev. 1). National Institute of Standards and Technology.

Souppaya, M., & Scarfone, K. (2013). Guide to *Malware Incident Prevention and Handling for Desktops and Laptops* (NIST Special Publication 800-83 Revision 1). National Institute of Standards and Technology.

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th Edition). Pearson Education.

Susanto, E. *et al.* (2023) 'Manajemen Keamanan Cyber di Era Digital', *Journal of Business and Entrepreneurship*, 11(1), pp. 23–33. Available at: <https://doi.org/10.46273/job&e.v11i1.365>.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Towidjojo, R. (2019). MikroTik Kung Fu: Kitab 1 (Edisi Terbaru). Jasakom.

Van Rossum, G., & Drake, F. L. (2009). Python 3 Reference Manual. CreateSpace.

Wazuh Inc (2025) *Active Response*, *Wazuh Documentation*. Available at: <https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html#active-response> (Accessed: 16 December 2025).

Wazuh Inc. (2025) *Getting started with Wazuh*, *Wazuh Documentation*. Available at: <https://documentation.wazuh.com/current/getting-started/index.html> (Accessed: 16 December 2025).





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR RIWAYAT HIDUP



Bayu Dwi Setianto

Saya lahir dan bertumbuh di Depok pada tahun 2003. Menjadi putra dari pasangan Bapak Jumangat dan Ibu Sumiyati adalah sebuah anugerah kebanggaan tersendiri bagi saya. Dukungan penuh, kasih sayang, serta doa yang tak pernah putus dari kedua orang tua senantiasa menjadi pijakan sekaligus motivasi terkuat saya dalam melangkah melewati setiap fase kehidupan dan pendidikan. Perjalanan akademis saya seluruhnya dihabiskan di kota kelahiran tercinta ini. Saya menamatkan pendidikan dasar di MI Nurul Huda pada tahun 2016, kemudian melanjutkannya ke MTs Negeri 1 Depok hingga lulus pada tahun 2019. Masa putih abu-abu pun saya selesaikan di SMK Negeri 3 Depok pada tahun 2022. Berbekal ketertarikan yang mendalam terhadap dunia teknologi informasi, khususnya dalam ranah infrastruktur dan keamanan jaringan, saya memutuskan untuk melanjutkan pendidikan ke jenjang Diploma Empat (D4) pada Program Studi Teknik Multimedia dan Jaringan. Selama masa perkuliahan, saya tidak hanya berfokus pada teori di dalam kelas, tetapi juga aktif mengembangkan kapasitas diri. Saya diberikan kepercayaan untuk mengemban tanggung jawab sebagai asisten dosen, sebuah pengalaman yang sangat mengasah kemampuan komunikasi dan pendalaman materi teknis saya. Selain itu, pada tahun 2023, saya juga berkesempatan untuk merancang dan mengembangkan sistem smart CCTV serta sistem absensi pintar berbasis pengenalan wajah. Saya menyadari bahwa ilmu yang bermanfaat adalah ilmu yang dibagikan. Oleh karena itu, pada tahun 2024, saya turut serta dalam kegiatan pengabdian masyarakat di Sekolah Alam Indonesia Cibinong sebagai bentuk implementasi langsung dan kontribusi sosial kepada masyarakat.

Kini, penyusunan skripsi ini tidak hanya menjadi penutup dari rangkaian perjalanan akademis saya di kampus, tetapi juga saya yakini sebagai gerbang awal untuk melangkah lebih jauh dan memberikan kontribusi yang nyata di industri keamanan siber.



LAMPIRAN

Lampiran 1 Konfigurasi Ossec.conf Wazuh Manager

```
<command>
  <name>remove-threat</name>
  <executable>remove-threat</executable>
  <timeout_allowed>no</timeout_allowed>
</command>

<active-response>
  <disabled>no</disabled>
  <command>remove-threat</command>
  <location>all</location>
  <rules_id>100002,100500</rules_id>
</active-response>

<command>
  <name>block-mikrotik</name>
  <executable>block-mikrotik</executable>
  <timeout_allowed>no</timeout_allowed>
</command>

<active-response>
  <disabled>no</disabled>
  <command>block-mikrotik</command>
  <location>defined-agent</location>
  <agent_id>001</agent_id>
  <rules_id>100501</rules_id>
</active-response>

<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <list>etc/lists/malware-hashes</list>

  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>
</ruleset>

<ossec_config>
  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>audit</log_format>
    <location>/var/log/audit/audit.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/chimera_soar.json</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/chimera_cti.json</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/chimera_ip.json</location>
  </localfile>
</ossec_config>
```

Lampiran 2 Log Chimera_CTI

```
{
  "timestamp": "2026-06-08T04:07:13.836253",
  "target": {
    "file_hash": "275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd0f",
    "filename": "eicar.com.txt",
    "path": "/home/agent/Downloads/eicar.com.txt",
    "src_ip": "127.0.0.1",
    "dst_ip": "127.0.0.1",
    "agent_id": "010",
    "score": {
      "final_score": 0.33,
      "status": "MALICIOUS",
      "severity": "high"
    },
    "details": {
      "source": "fim",
      "vt_hash_norm": 0.9706,
      "ctx_hash_norm": 0.0,
      "otx_severity": "50 pulses score:6 Medium Risk",
      "ctx_name": null,
      "hash_score": 0.33,
      "hash_status": "MALICIOUS",
      "hash_severity": "high"
    }
  },
  "timestamp": "2026-06-08T04:08:45.182215",
  "target": {
    "file_hash": "275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd0f",
    "filename": "eicar.com.txt",
    "path": "/home/agent/Downloads/eicar.com.txt",
    "src_ip": "127.0.0.1",
    "dst_ip": "127.0.0.1",
    "agent_id": "010",
    "score": {
      "final_score": 0.33,
      "status": "MALICIOUS",
      "severity": "high"
    },
    "details": {
      "source": "fim",
      "vt_hash_norm": 0.9706,
      "ctx_hash_norm": 0.0,
      "otx_severity": "50 pulses score:6 Medium Risk",
      "ctx_name": null,
      "hash_score": 0.33,
      "hash_status": "MALICIOUS",
      "hash_severity": "high"
    }
  },
  "timestamp": "2026-06-08T04:08:45.280317",
  "target": {
    "file_hash": "275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd0f",
    "filename": "eicar.com.txt",
    "path": "/home/agent/Downloads/eicar.com.txt",
    "src_ip": "127.0.0.1",
    "dst_ip": "127.0.0.1",
    "agent_id": "010",
    "score": {
      "final_score": 0.33,
      "status": "MALICIOUS",
      "severity": "high"
    },
    "details": {
      "source": "fim",
      "vt_hash_norm": 0.9706,
      "ctx_hash_norm": 0.0,
      "otx_severity": "50 pulses score:6 Medium Risk",
      "ctx_name": null,
      "hash_score": 0.33,
      "hash_status": "MALICIOUS",
      "hash_severity": "high"
    }
  },
  "timestamp": "2026-06-08T04:14:01.144276",
  "target": {
    "file_hash": "1cb988180bd80475996c6866b1d28d5b1faf8830b5d61d61b6ecc7577b6b4b2c",
    "filename": "ai_sample1",
    "path": "/home/agent/Downloads/ai_sample1",
    "src_ip": "127.0.0.1",
    "dst_ip": "127.0.0.1",
    "agent_id": "010",
    "score": {
      "final_score": 0.0,
      "status": "NORMAL",
      "severity": "low"
    },
    "details": {
      "source": "fim",
      "vt_hash_norm": 0.0,
      "ctx_hash_norm": 0.0,
      "otx_severity": "none",
      "ctx_name": null,
      "hash_score": 0.0,
      "hash_status": "NORMAL",
      "hash_severity": "low"
    }
  }
}
```



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 3 Log Chimea_SOAR

```
{
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "154.52.16.195"
      }
    }
  },
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "154.52.16.195"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/eicar.com.txt",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/eicar.com.txt",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "89.238.73.97"
      }
    }
  },
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "89.238.73.97"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/eicar.com.txt",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/eicar.com.txt",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "89.238.73.97"
      }
    }
  },
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "89.238.73.97"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/eicar.com.txt",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/eicar.com.txt",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/ai_sample1",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/ai_sample1",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "block-mikrotik",
    "data": {
      "target": {
        "src_ip": "154.52.16.195"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/ai_sample1",
        "agent_id": "010"
      }
    }
  },
  "chimera": {
    "action": "remove-threat",
    "data": {
      "target": {
        "path": "/home/agent/Downloads/ai_sample1",
        "agent_id": "010"
      }
    }
  }
}
```

Lampiran 4 Hash_Scanning.py

```
#!/bin/bash

if [ "$EUID" -ne 0 ]; then
  echo "[ ] ERROR: Harap jalankan script ini sebagai root (Gunakan sudo)"
  exit 1
fi

echo "[+] Memulai inialisasi sistem terintegrasi..."
systemctl stop suricata 2>/dev/null
pkill -f "PolarProxy" 2>/dev/null
pkill -f "nc localhost 57012" 2>/dev/null
pkill -f "tcpreplay -i dec0" 2>/dev/null
pkill -f "chimera_filter.sh" 2>/dev/null
pkill -f "tail -F /var/log/suricata/eve.json" 2>/dev/null

sysctl -w net.ipv4.ip_forward=1 > /dev/null
sysctl -w net.ipv4.conf.all.send_redirects=0 > /dev/null
sysctl -w net.ipv4.conf.default.send_redirects=0 > /dev/null

modprobe dummy
ip link add name dec0 type dummy 2>/dev/null
ip link set dec0 up

iptables -t nat -D PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 10443 2>/dev/null
iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 10443

nohup /opt/PolarProxy/PolarProxy -p 10443,80,443 -x /opt/PolarProxy/polarproxy.cer --pcapoverip 57012 > /var/log/polarproxy.log 2>&1 &
sleep 2
nohup sh -c 'while true; do nc localhost 57012 | tcpreplay -i dec0 -t -; sleep 1; done' > /dev/null 2>&1 &

echo "[+] Menjalankan Suricata NIDS pada interface dec0..."
nohup suricata -c /etc/suricata/suricata.yaml -i dec0 > /var/log/suricata_dec0.log 2>&1 &

echo "[+] Membangun mesin diet log (eve_filtered.json) untuk Wazuh..."
> /var/log/suricata/eve_filtered.json

cat << 'EOF' > /tmp/chimera_filter.sh
#!/bin/bash
tail -F /var/log/suricata/eve.json | grep --line-buffered '"event_type":"fileinfo"' | while read -r line; do
  echo "$line" | jq -c 'select(.fileinfo.sha256 != null)' >> /var/log/suricata/eve_filtered.json
done
EOF

chmod +x /tmp/chimera_filter.sh
nohup /tmp/chimera_filter.sh > /dev/null 2>&1 &

echo "=====
[V] SISTEM CHIMERA (SURICATA + WAZUH FILTER) BERHASIL DIJALANKAN
====="
```



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 6 Rules.xml

```

1 <group name="chimera_cti,">
2
3 <rule id="100600" level="3">
4   <decoded_as>json</decoded_as>
5   <field name="scores.status" type="pcre2">.+</field>
6   <description>Chimera CTI: Log analisis reputasi diterima.</description>
7 </rule>
8
9 <rule id="100101" level="7">
10  <if_sid>100600</if_sid>
11  <field name="scores.status">SUSPICIOUS</field>
12  <description>Chimera CTI: File $(target.filename) MENCURIGAKAN (Skor: $(scores.final_score))</description>
13  <mitre>
14    <id>T1204.002</id>
15  </mitre>
16 </rule>
17
18 <rule id="100102" level="12">
19  <if_sid>100600</if_sid>
20  <field name="scores.status">MALICIOUS</field>
21  <description>Chimera CTI: TERDETEKSI MALWARE! File: $(target.filename) | Hash: $(target.file_hash)</description>
22  <mitre>
23    <id>T1588.002</id>
24  </mitre>
25 </rule>
26
27 <rule id="100103" level="3">
28  <if_sid>100600</if_sid>
29  <field name="scores.status">NORMAL</field>
30  <description>Chimera CTI: File $(target.filename) dinyatakan aman.</description>
31 </rule>
32
33 </group>
34
35 <group name="local,malware,">
36
37 <rule id="100002" level="12">
38  <if_sid>554, 550</if_sid>
39  <list field="sha256" lookup="match_key">etc/lists/malware-hashes</list>
40  <description>CDB Hashes list: File terindikasi Blacklist terdeteksi: $(file)</description>
41  <mitre>
42    <id>T1204.002</id>
43  </mitre>
44 </rule>
45
46 <rule id="100003" level="5">
47  <if_sid>100002</if_sid>
48  <field name="file" type="pcre2">(?!)[c-z]:</field>
49  <description>A file - $(file) - malware blacklist ditambahkan ke sistem.</description>
50 </rule>
51
52 </group>
53
54 <group name="chimera_soar,">
55
56 <rule id="100100" level="3">
57  <decoded_as>json</decoded_as>
58  <field name="chimera.action" type="pcre2">.+</field>
59  <description>SOAR: Log Active-Response diterima.</description>
60 </rule>
61
62 <rule id="100500" level="12">
63  <if_sid>100100</if_sid>
64  <field name="chimera.action">remove-threat</field>
65  <description>SOAR: Mengeksekusi penghapusan malware.</description>
66 </rule>
67
68 <rule id="100501" level="12">
69  <if_sid>100100</if_sid>
70  <field name="chimera.action">block-mikrotik</field>
71  <description>SOAR: Mengeksekusi blokir IP Penyerang di MikroTik.</description>
72 </rule>
73
74 </group>
75
76 <group name="suricata, chimera_nids,">
77 <rule id="100250" level="5">
78  <if_sid>86600</if_sid>
79  <field name="event_type">^fileinfo$</field>
80  <field name="fileinfo.sha256">\.+.</field>
81  <description>CHIMERA NIDS: Ekstraksi File Terdeteksi dari Jaringan (Hash: $(fileinfo.sha256))</description>
82 </rule>
83 </group>

```



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 7 Block-mikrotik

```

1  #!/home/ubuntu/Surcata-IDS-IPS/venv/bin/python
2
3  import sys
4  import json
5  import datetime
6  import os
7
8  try:
9      import routeros_api
10 except ImportError:
11     routeros_api = None
12
13 # --- KONFIGURASI MIKROTIK ---
14 MIKROTIK_IP = "192.168.11.1"
15 MIKROTIK_USER = "admin"
16 MIKROTIK_PASS = ""
17 MIKROTIK_PORT = 8728
18 ADDRESS_LIST_NAME = "suricata_blocklist"
19
20 LOG_FILE = "/var/ossec/logs/active-responses.log"
21
22 def write_log(msg):
23     """Menulis log aktivitas skrip Active Response."""
24     waktu = datetime.datetime.now().strftime('%Y/%m/%d %H:%M:%S')
25     with open(LOG_FILE, mode="a") as f:
26         f.write(f"{waktu} block-mikrotik: {msg}\n")
27
28 def block_ip(ip_address):
29     """Terhubung ke MikroTik via API dan menambahkan IP ke Address List."""
30     if routeros_api is None:
31         write_log("GAGAL: Library 'routeros_api' belum terinstal di virtual environment (venv)!")
32         return
33
34     write_log(f"Mencoba memblokir IP: {ip_address} di MikroTik ({MIKROTIK_IP})...")
35
36     try:
37         connection = routeros_api.RouterOsApiPool(
38             MIKROTIK_IP,
39             username=MIKROTIK_USER,
40             password=MIKROTIK_PASS,
41             port=MIKROTIK_PORT,
42             plaintext_login=True
43         )
44         api = connection.get_api()
45
46         address_list = api.get_resource('/ip/firewall/address-list')
47         exists = address_list.get(address=ip_address, list=ADDRESS_LIST_NAME)
48
49         if not exists:
50             address_list.add(
51                 list=ADDRESS_LIST_NAME,
52                 address=ip_address,
53                 comment="SOAR: Otomatis diblokir karena deteksi malware jaringan"
54             )
55             write_log(f"IP {ip_address} berhasil diblokir Permanen!")
56         else:
57             write_log(f"IP {ip_address} sudah ada di daftar blokir MikroTik. Diabaikan.")
58
59         connection.disconnect()
60
61     except Exception as e:
62         write_log(f"GAGAL: Terjadi kesalahan saat berkomunikasi dengan MikroTik: {e}")
63
64 def main():
65     write_log("=== SKRIP BLOKIR MIKROTIK BERJALAN ===")
66
67     try:
68         for line in sys.stdin:
69             input_str = line.strip()
70             if not input_str:
71                 continue
72
73             try:
74                 data = json.loads(input_str)
75             except Exception as e:
76                 write_log(f"Error parsing JSON: {e}")
77                 continue

```



(Lanjutan)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

72
73     try:
74         data = json.loads(input_str)
75     except Exception as e:
76         write_log(f"Error parsing JSON: {e}")
77         continue
78
79     command = data.get("command")
80
81     if command == "check_keys":
82         print(json.dumps({"error": 0, "message": "Keys checked"}))
83         sys.stdout.flush()
84         continue
85
86     if command == "add":
87         target_ip = None
88         parameters = data.get("parameters", {})
89         alert_data = parameters.get("alert", {})
90
91         target_ip = alert_data.get("data", {}).get("srcip")
92         if not target_ip:
93             target_ip = alert_data.get("data", {}).get("src_ip")
94
95         if not target_ip:
96             target_ip = alert_data.get("data", {}).get("data", {}).get("target", {}).get("src_ip")
97
98         if not target_ip:
99             write_log("GAGAL: Alamat IP (src_ip) tidak ditemukan di dalam log JSON.")
100         elif target_ip in ["127.0.0.1", "0.0.0.0", "localhost"]:
101             write_log(f"DITOLAK: Upaya memblokir IP lokal ({target_ip}) dicegah.")
102         else:
103             block_ip(target_ip)
104
105         print(json.dumps({"error": 0, "message": "Active response completed"}))
106         sys.stdout.flush()
107         return
108
109     except Exception as e:
110         write_log(f"FATAL ERROR: {str(e)}")
111
112 if __name__ == "__main__":
113     main()
114

```

Lampiran 8 Remove-threat

```

1  #!/usr/bin/python3
2  import sys
3  import json
4  import os
5  from datetime import datetime
6  LOG_FILE = "/var/ossec/logs/active-responses.log"
7
8  def write_log(message):
9      """Mencetak log aktivitas skrip Active Response."""
10     timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')
11     with open(LOG_FILE, "a") as f:
12         f.write(f"[timestamp] remove-threat: {message}\n")
13
14 def get_local_agent_id():
15     """Membaca ID agen lokal dari file konfigurasi Wazuh (Safety Lock)."""
16     try:
17         if os.path.exists("/var/ossec/etc/client.keys"):
18             with open("/var/ossec/etc/client.keys", "r") as f:
19                 return f.readline().split(" ")[0]
20     except Exception:
21         pass
22     return "000"
23
24 def main():
25     write_log("Menerima pemicu Active Response. Skrip mulai berjalan...")
26
27     try:
28         for line in sys.stdin:
29             input_data = line.strip()
30             if not input_data:
31                 continue
32

```



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

33     ar_data = json.loads(input_data)
34     command = ar_data.get("command")
35
36     if command == "check_keys":
37         print(json.dumps({"error": 0, "message": "Keys checked"}))
38         sys.stdout.flush()
39         continue
40
41     if command == "add":
42         parameters = ar_data.get("parameters", {})
43         alert = parameters.get("alert", {})
44         rule_id = alert.get("rule", {}).get("id", "Unknown")
45
46         write_log(f"INFO: Dipicu oleh Rule ID -> {rule_id}")
47
48         target_path = None
49         soar_target_id = None
50
51         syscheck_block = alert.get("syscheck", {})
52         if "path" in syscheck_block:
53             target_path = syscheck_block.get("path")
54
55         else:
56             custom_data = alert.get("data", {}).get("data", {})
57             target_path = custom_data.get("target", {}).get("path")
58             soar_target_id = custom_data.get("target", {}).get("agent_id")
59
60         if soar_target_id:
61             my_agent_id = get_local_agent_id()
62             if soar_target_id != my_agent_id:
63                 write_log(f"INFO: Abaikan perintah. Target adalah Agen {soar_target_id}, tapi saya Agen {my_agent_id}.")
64
65                 print(json.dumps({"error": 0, "message": "Ignored, broadcast targeted another agent"}))
66                 sys.stdout.flush()
67                 return
68
69         if target_path:
70             write_log(f"Target ditemukan. Bersiap menghapus file: {target_path}")
71
72             if os.path.exists(target_path):
73                 os.remove(target_path)
74                 write_log(f"SUKSES: Ancaman pada {target_path} telah dihancurkan!")
75             else:
76                 write_log(f"INFO: File {target_path} tidak ditemukan (Mungkin sudah terhapus FIM).")
77
78         else:
79             write_log("ERROR: Variabel 'path' tidak ditemukan di dalam log JSON.")
80             write_log(f"DEBUG Dump JSON: {input_data}")
81
82         print(json.dumps({"error": 0, "message": "Active response completed"}))
83         sys.stdout.flush()
84         return
85
86     except json.JSONDecodeError:
87         write_log("ERROR: Format input bukan JSON yang valid.")
88     except Exception as e:
89         write_log(f"ERROR FATAL: {str(e)}")
90
91 if __name__ == "__main__":
92     main()

```