

**IMPLEMENTASI SIEM BERBASIS WAZUH DAN SNORT IDS
MENGUNAKAN FRAMEWORK MITRE ATT&CK PADA
JARINGAN DMZ**

TUGAS AKHIR

Untuk memenuhi sebagai persyaratan

Mencapai derajat Sarjana S-1

Program Studi Informatika



**PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA
2026**

LEMBAR PENGESAHAN



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI

Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1381/Un.02/DST/PP.00.9/06/2026

Tugas Akhir dengan judul : IMPLEMENTASI SIEM BERBASIS WAZUH DAN SNORT IDS MENGGUNAKAN
FRAMEWORK MITRE ATT&CK PADA JARINGAN DMZ

yang dipersiapkan dan disusun oleh:

Nama : MUHAMMAD FARIS BAKRI
Nomor Induk Mahasiswa : 22106050025
Telah diujikan pada : Jumat, 05 Juni 2026
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR



Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 6a3baf134c898



Penguji I

Ir. Muhammad Taufiq Nuruzzaman, S.T.
M.Eng., Ph.D.
SIGNED

Valid ID: 6a27ad135c247



Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 6a3b6c699c26



Yogyakarta, 05 Juni 2026
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi
Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6a422bb51021b

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Faris Bakri
NIM : 22106050025
Program Studi : Informatika
Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya, bahwa skripsi saya yang berjudul
"IMPLEMENTASI SIEM BERBASIS WAZUH DAN SNORT IDS
MENGUNAKAN FRAMEWORK MITRE ATT&CK PADA JARINGAN
DMZ" merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis,
bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang
penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar,
sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 10 Mei 2026

METERAI
TEMPEL
AT1B0A0X000653093

Muhammad Faris Bakri
22106050025

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

LEMBAR PERSETUJUAN



Universitas Islam Negeri Sunan Kalijaga



FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir

Lamp : -

Kepada

Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhammad Faris Bakri
NIM : 22106050025
Judul Skripsi : IMPLEMENTASI SIEM BERBASIS WAZUH DAN
SNORT IDS MENGGUNAKAN FRAMEWORK MITRE
ATT&CK PADA JARINGAN DMZ

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Yogyakarta, 19 Mei 2026

Pembimbing

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN

Eng.

NIP. 197510242009121002

INTISARI

Infrastruktur jaringan dan pusat data di PTIPD UIN Sunan Kalijaga mengelola berbagai layanan kritis yang rentan terhadap vektor ancaman siber berskala kompleks. Proses pemantauan keamanan pada perangkat yang heterogen, seperti *server* dan infrastruktur jaringan, seringkali masih bersifat terfragmentasi. Kondisi ini menyulitkan administrator dalam membedah data log mentah (*raw log*) dan mengkorelasikan anomali secara terpusat, sehingga berpotensi memperlambat waktu respons terhadap insiden. Penelitian ini bertujuan untuk merancang, mengimplementasikan, dan mengevaluasi sistem *Security Information and Event Management* (SIEM) terintegrasi yang mampu memusatkan visibilitas keamanan dan menerjemahkan log kejadian secara *real-time*.

Sistem dikembangkan menggunakan metode *Network Development Life Cycle* (NDLC) yang meliputi tahapan analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Arsitektur pemantauan dibangun menggunakan pendekatan *Out-of-Band Logging* pada lingkungan virtualisasi VMware vSphere, mengintegrasikan Wazuh sebagai pusat kendali SIEM dan Snort 3 sebagai sensor jaringan (*Network Intrusion Detection System*). Pengumpulan log diimplementasikan melalui metode berbasis agen (*agent-based*) pada sistem operasi *server*, serta nir-agen (*agentless*) menggunakan protokol Rsyslog untuk mengakomodasi perangkat *closed-system* seperti *switch* Ruckus ICX. Sistem ini juga diperkuat dengan rekayasa logika pemantauan melalui *Custom Decoder* dan aturan korelasi (*Parent-Child Rule*).

Hasil pengujian memvalidasi keandalan sistem dalam mendeteksi serangan siber proaktif yang merujuk pada standarisasi kerangka kerja MITRE ATT&CK. Sistem terbukti berhasil mengidentifikasi secara akurat seluruh skenario pengujian lintas lapisan, meliputi taktik *Discovery* (T1046), *Credential Access* (T1110), dan *Initial Access* (T1189, T1190). Lebih lanjut, mekanisme korelasi *ruleset* terbukti efektif membedakan anomali jaringan berskala kecil dengan serangan persisten (*Impact* - T1498), melalui eskalasi peringatan secara dinamis ke status kritis (Level 15). Evaluasi sistem juga membuktikan kemampuan ekstraksi visibilitas forensik (*Log Enrichment*) yang komprehensif dengan tingkat latensi pemrosesan *Near Real-Time*. Implementasi ini menghasilkan arsitektur pertahanan yang terpusat, terstandarisasi, dan berkelanjutan bagi ekosistem jaringan PTIPD.

Kata Kunci: SIEM, Wazuh, Snort3, MITRE ATT&CK, NDLC, Keamanan Jaringan.

ABSTRACT

The network infrastructure and data center at PTIPD UIN Sunan Kalijaga manage various critical services that are vulnerable to complex cyber threat vectors. The security monitoring process on heterogeneous devices, such as servers and network infrastructure, is often fragmented. This condition makes it difficult for administrators to parse raw log data and correlate anomalies centrally, potentially slowing down incident response times. This research aims to design, implement, and evaluate an integrated Security Information and Event Management (SIEM) system capable of centralizing security visibility and translating event logs in real-time.

The system was developed using the Network Development Life Cycle (NDLC) method, which includes analysis, design, simulation, implementation, monitoring, and management stages. The monitoring architecture is built using an Out-of-Band Logging approach on the VMware vSphere virtualization environment, integrating Wazuh as the SIEM control center and Snort 3 as the network sensor (Network Intrusion Detection System). Log collection is implemented through an agent-based method on server operating systems and an agentless approach using the Rsyslog protocol to accommodate closed-system devices such as the Ruckus ICX switch. The system is also enhanced by monitoring logic engineering through Custom Decoders and correlation rules (Parent-Child Rule).

The test results validate the system's reliability in proactively detecting cyber attacks referring to the MITRE ATT&CK framework standardization. The system proved successful in accurately identifying all cross-layer testing scenarios, including Discovery (T1046), Credential Access (T1110), and Initial Access (T1189, T1190) tactics. Furthermore, the ruleset correlation mechanism proved effective in distinguishing small-scale network anomalies from persistent attacks (Impact - T1498), characterized by the dynamic escalation of alerts to critical status (Level 15). The system evaluation also demonstrated comprehensive forensic visibility extraction (Log Enrichment) capabilities with Near Real-Time processing latency. This implementation produces a centralized, standardized, and sustainable defense architecture for the PTIPD network ecosystem..

Keywords: SIEM, Wazuh, Snort, MITRE ATT&CK, NDLC, Network Security..

MOTTO

*“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.” — **Gene Spafford***



HALAMAN PERSEMBAHAN

Atas berkah dan rahmat Tuhan Yang Maha Esa tugas akhir ini penulis persembahkan kepada :

Muhammad Nizaar dan Arie Yani Nobelia

Orang tua penulis

Semua Keluarga Penulis

Semua Saudara, Sahabat, dan Teman Penulis

Semua rekan PT. Winder Baby Indonesia

Semua rekan PT.Begja Jaya Abadi

Yang selalu memberikan dukungan dan masukan kepada penulis

Dan

Almamater Tercinta

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
Program Studi Informatika Fakultas Sains dan Teknologi
UIN Sunan Kalijaga
YOGYAKARTA

PENGANTAR

Puji syukur penulis haturkan kepada Tuhan Yang Maha Esa Allah SWT, karena berkah rahmat dan hidayah-Nya penulis dapat menyelesaikan penulisan tugas akhir yang berjudul “Implementasi SIEM Berbasis Wazuh dan Snort IDS Menggunakan Framework Mitre Att&ck Pada Jaringan DMZ”.

Tugas akhir ini dibuat untuk memenuhi salah satu persyaratan untuk memperoleh gelar Sarjana Strata 1 di program studi Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga Yogyakarta.

Penulis menyadari bahwa tugas akhir ini masih jauh dari kesempurnaan. Oleh sebab itu, penulis berharap dapat belajar banyak dalam menerapkan ilmu yang didapatkan. Tugas akhir ini tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini saya ingin mengucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Prof. Noorhaidi Hasan, S.Ag., M.A., M.Phil., Ph.D., selaku rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
3. Bapak Dr. Muhammad Mustakim, S.T. M.T., selaku ketua program studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
4. Bapak Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng., selaku dosen pembimbing akademik penulis.
5. Ibu Siti Mutmainah, S.Kom., M.Cs., Ph.D., selaku Kepala UPT.PTIPD UIN Sunan Kalijaga.

6. Bapak Frendi Yusroni Romadhona, S.Kom. M.Kom., Anggota Divisi Infrastruktur dan Keamanan Informasi UPT. PTIPD selaku pembimbing teknis penulis.
7. Bapak Eryan Yogi Arifianto, S.Kom. M.Kom., Sekretaris UPT. PTIPD selaku pembimbing teknis penulis.
8. Orang tua tercinta Bapak Muhammad Nizaar, Ibu Arie Yani Nobelia, Khafidlotul Khoiriyah, Muhimmi.
9. Seluruh saudara kandung dan tiri penulis.
10. Bapak Mohammad Wildan Yonaizar selaku Owner PT.Winder Baby Indonesia.
11. Diva Septiana Putri sebagai partner penyemangat dalam penulisan tugas akhir bagi penulis.
12. Rekan-rekan PT. Winder Baby Indonesia & PT Begja Jaya Abadi.
13. Teman-teman KKN Dusun Jurug sebagai tempat berkumpulnya orang-orang ambisius di Informatika UIN.
14. Semua pihak yang telah membantu yang tidak dapat penulis sebutkan satu persatu.

Saya berharap semoga Tuhan Yang Maha Esa mengaruniakan rahmat dan hidayah-Nya kepada mereka semua. Semoga tugas akhir ini dapat bermanfaat bagi kita semua.

Yogyakarta, 10 Mei 2026

Penulis,

Muhammad Faris Bakri

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN KEASLIAN.....	iii
LEMBAR PERSETUJUAN	iv
INTISARI	v
ABSTRACT	vi
MOTTO	vii
HALAMAN PERSEMBAHAN	viii
PENGANTAR	viii
DAFTAR ISI.....	xi
DAFTAR TABEL	xiv
DAFTAR GAMBAR.....	xv
BAB I PENDAHULUAN	1
1. 1 Latar Belakang.....	1
1. 2 Rumusan Masalah.....	5
1. 3 Batasan Masalah	6
1. 4 Manfaat Penelitian	8
1. 5 Tujuan Penelitian	10
BAB II KAJIAN PUSTAKA DAN LANDASAN TEORI.....	11
2. 1 Kajian Pustaka	11
2. 2 Landasan Teori.....	16
2.2.1. Jaringan DMZ.....	16
2.2.2. SIEM.....	17
2.2.3. Wazuh	17
2.2.4. Snort 3.....	18
2.2.5. MITRE ATT&CK.....	19
2.2.6. Rsyslog	20

2.2.7. Sistem Operasi Berbasis Linux.....	20
BAB III METODE PENGEMBANGAN SISTEM.....	22
3. 1 Metode Pengembangan Sistem.....	22
3. 2 Tahapan Penelitian.....	23
3.2.1. Analysis	23
3.2.2. Design.....	25
3.2.3. Simulation.....	32
3.2.4. Implementation.....	33
3.2.5. Monitoring.....	36
3.2.6. Management	38
BAB IV PERANCANGAN DAN EVALUASI SISTEM	39
4. 1 Implementasi Perancangan Sistem	39
4.1.1 Implementasi Server SIEM Terpusat.....	39
4.1.2 Konfigurasi Wazuh Agent dan Host-based IDS	41
4.1.3 Konfigurasi Layanan Web Tiruan (Dummy SIA).....	43
4.1.4 Konfigurasi Rsyslog Pada Infrastruktur Jaringan.....	45
4.1.5 Implementasi Manajemen dan Pemeliharaan Sistem	46
4. 2 Hasil Integrasi dan Konfigurasi Logika Sistem.....	47
4.2.1 Integrasi Wazuh Agent dan Wazuh Server.....	47
4.2.2 Konfigurasi Custom Decoder dan Aturan Korelasi.....	49
4. 3 Analisis dan Pengujian Sistem.....	52
4.3.1 Skenario Pengujian Discovery (T1046 - Network Scanning).....	53
4.3.2 Skenario Pengujian Credential Access (T1110 - Brute Force)	54
4.3.3 Skenario Pengujian Initial Access (T1189-T1190).....	57
4.3.4 Skenario Pengujian Impact (T1498 - Denial of Service)	59
4. 4 Hasil Evaluasi Sistem	61

4.4.1	Evaluasi Kelengkapan Visibilitas Forensik (<i>Log Enrichment</i>)	63
4.4.2	Evaluasi Latensi Deteksi (<i>Near Real-Time Monitoring</i>)	64
BAB V PENUTUP		67
5.1	Kesimpulan	67
5.2	Saran	68
DAFTAR PUSTAKA		71
LAMPIRAN		75



DAFTAR TABEL

Tabel 3. 1 Tabel Segmentasi Zona dan Peran Infrastruktur	27
Tabel 3. 2 Matriks Skenario Pengujian (Berdasarkan MITRE ATT&CK)	37
Tabel 4. 1 Hasil Evaluasi Deteksi Serangan (Berdasarkan MITRE ATT&CK)	61
Tabel 4. 2 Hasil Evaluasi Ekstraksi Variabel Forensik	63
Tabel 4. 3 Evaluasi Waktu Latensi Deteksi	65



DAFTAR GAMBAR

Gambar 3.1 Siklus Diagram Network Development	22
Gambar 3. 2 Gambar Serangan pada NGFW PTIPD.....	24
Gambar 3. 3 Topologi Jaringan PTIPD UIN Sunan.....	26
Gambar 3. 4 Desain Arsitektur WazuhAll in One(Single Node)	28
Gambar 3. 5 Desain Integrasi Log Multi-Sumber dan Rsyslog.....	29
Gambar 3. 6 Desain Alur NIDS Snort3.....	30
Gambar 3. 7 Desain Alur Pemantauan Aplikasi Web.....	31
Gambar 4. 1 Status Layanan Inti Wazuh pada Server Rocky Linux.....	40
Gambar 4. 2 Halaman Web Wazuh Dashboard	40
Gambar 4. 3 Status Wazuh Agent pada Ubuntu Server.....	41
Gambar 4. 4 Konfigurasi ossec.conf pada Wazuh Agent.....	42
Gambar 4. 5 Konfigurasi Parameter HOME_NET	43
Gambar 4. 6 Forwarding Log Snort3 pada berkas /var/log/snort/alert_fast.txt	43
Gambar 4. 7 UI Layanan Web Dummy.....	44
Gambar 4. 8 Konfigurasi Rsyslog pada server Ubuntu.....	46
Gambar 4. 9 Integrasi Real-time Log Ruckus pada server Ubuntu	46
Gambar 4. 10 Status Wazuh Agent Ubuntu pada Wazuh Dasboard.....	48
Gambar 4. 11 Visualisasi auth.log dari Agen Ubuntu pada Wazuh Dashboard.....	49
Gambar 4. 12 Konfigurasi Custom Decoder pada Wazuh Manager	50
Gambar 4. 13 Konfigurasi Custom Rules pada Wazuh Manager	51
Gambar 4. 14 Visualisasi Log Ruckus pada Wazuh Dashboard	52
Gambar 4. 15 Visualisasi Log Snort3 pada Wazuh Dashboard.....	52
Gambar 4. 16 Pengujian Nmap pada Ubuntu Server menggunakan Kali Linux.....	53
Gambar 4. 17 Visualisasi Deteksi Aktivitas Discovery(Level 10) pada Antarmuka Wazuh Dashboard.....	54
Gambar 4. 18 Pengujian Hydra dan Deteksi Kegagalan Autentikasi SSH Ubuntu pada Wazuh Dashboard	55

Gambar 4. 19 Pengujian Bash Script SSH dan Hasil Deteksi pada Wazuh Dashboard.....	56
Gambar 4. 20 Pengujian Bash Script SNMP dan Hasil Deteksi pada Wazuh Dashboard.....	57
Gambar 4. 21 Pengujian SQL Injection dan XSS Script pada Web Dummy	58
Gambar 4. 22 Hasil Deteksi SQL Injection dan XSS Scripting pada Wazuh Dashboard.....	59
Gambar 4. 23 Pengujian Dos pada Ubuntu Server	60
Gambar 4. 24 Hasil Deteksi Serangan DoS pada Wazuh Dashboard	60



BAB I

PENDAHULUAN

1. 1 Latar Belakang

Kehadiran infrastruktur jaringan dan teknologi informasi dalam dekade terakhir telah menjadi pilar fundamental yang menggerakkan operasional di berbagai sektor. Kelancaran proses transformasi digital ini sangat bergantung pada interkoneksi digital global yang beroperasi secara terus-menerus. Namun, akselerasi ini secara signifikan berbanding lurus dengan peningkatan risiko serta eskalasi ancaman siber yang kian masif, yang tidak lagi sekadar menyebabkan gangguan layanan, melainkan berujung pada pencurian data kritis (data breach) dan kerugian finansial berskala besar [1]. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2024, lanskap keamanan siber Indonesia mencatat angka yang sangat mengkhawatirkan dengan jumlah anomali lalu lintas internet mencapai lebih dari 330 juta kasus [2]. Berbagai anomali serangan ini didominasi oleh aktivitas Distributed Denial of Service (DDoS), eksploitasi malware, insiden web defacement, hingga infeksi ransomware [2]. Tingginya ancaman persisten ini menegaskan perlunya transformasi postur keamanan infrastruktur jaringan secara komprehensif.

Dalam arsitektur jaringan skala enterprise, pemisahan area keamanan umum diterapkan secara ketat untuk melindungi aset-aset kritis. Pendekatan arsitektural yang lazim digunakan adalah pembentukan Demilitarized Zone (DMZ) yang berfungsi sebagai zona penyangga (buffer zone) untuk mengisolasi jaringan publik eksternal

dari jaringan privat internal [3]. Untuk membatasi akses pada area ini, mayoritas organisasi masih sangat bergantung pada penggunaan perangkat Next-Generation Firewall (NGFW) maupun sistem keamanan perimeter konvensional [4]. Akan tetapi, mengandalkan pertahanan batas terluar semata kini dinilai tidak lagi memadai dalam menghadapi evolusi serangan modern. Firewall pada dasarnya dirancang untuk menyaring paket berdasarkan aturan statis di batas jaringan, sehingga memiliki titik buta (blind spot) yang sangat signifikan terhadap ancaman dari dalam (insider threat) [4]. Ketidadaan visibilitas di belakang dinding perimeter ini berisiko menyebabkan kegagalan sistem dalam mendeteksi pergerakan lateral (lateral movement) apabila penyerang telah berhasil memanipulasi kredensial yang sah atau menembus pertahanan awal [4].

Sebagai respons terhadap kompleksitas ancaman tersebut, studi kasus penelitian ini dilakukan pada infrastruktur jaringan Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas Islam Negeri (UIN) Sunan Kalijaga. Tingginya risiko keamanan di lingkungan akademik ini dibuktikan secara empiris melalui pemantauan dasbor Next-Generation Firewall (NGFW) milik PTIPD yang mencatat intensitas gempuran siber secara sangat masif. Dalam periode pemantauan 24 jam terakhir, sistem merekam total 26.877 kejadian intrusi (Intrusion Events), di mana 15.099 upaya di antaranya merupakan paket berbahaya yang berhasil diidentifikasi dan digugurkan (Dropped/Blocked). Tingginya angka lalu lintas anomali harian ini memberikan indikasi yang jelas bahwa risiko pembobolan perimeter bukanlah sebuah probabilitas semata, melainkan ancaman riil

yang sangat nyata. Apabila perimeter NGFW tersebut pada akhirnya berhasil ditembus, infrastruktur jaringan PTIPD memiliki kerentanan arsitektural yang kritis. Kampus menerapkan kebijakan jaringan multi-zona (multizone network) untuk menjamin kelancaran proses bisnis operasional dan mobilitas akademik, salah satunya adalah dukungan terhadap layanan jaringan nirkabel terintegrasi Eduroam [5], [6]. Kebijakan ini secara teknis mengharuskan adanya konektivitas komunikasi langsung antara segmen Local Area Network (LAN) yang berisi perangkat pengguna dengan segmen server yang berada di area DMZ. Kondisi interkoneksi ini secara tidak langsung merusak konsep isolasi Zero Trust murni, memperluas area permukaan serangan (Attack Surface), dan membuka celah kerentanan baru. Jika sebuah perangkat komputasi milik mahasiswa atau staf di jaringan LAN terinfeksi perangkat perusak, maka musuh dapat mengeksploitasi konektivitas tersebut untuk melakukan Lateral Movement ke server-server kritis di DMZ secara leluasa tanpa memicu peringatan dari keamanan perimeter luar [4].

Guna mengatasi titik buta arsitektural tersebut tanpa mengganggu proses bisnis akademik yang berjalan, diperlukan implementasi teknologi Security Information and Event Management (SIEM) berlapis yang andal. Pada lapisan pengawasan lalu lintas data, sistem membutuhkan sensor Network Intrusion Detection System (NIDS) seperti Snort versi 3 yang secara tangguh mampu melakukan Deep Packet Inspection untuk mengendus anomali protokol dan mengenali muatan eksploitasi di dalam aliran jaringan [7]. Sensor NIDS tersebut mutlak harus dipadukan dengan Wazuh, sebuah platform SIEM sumber terbuka yang bertindak secara komprehensif sebagai

Host-based Intrusion Detection System (HIDS) [8]. Wazuh dilengkapi dengan kapabilitas File Integrity Monitoring (FIM) yang sangat esensial untuk memberikan visibilitas titik akhir (endpoint) melalui pemantauan perubahan file sistem secara seketika, sekaligus bertindak sebagai mesin pengkorelasi log sentral (log correlator) dari berbagai perangkat di ekosistem DMZ [9]. Kolaborasi HIDS dan NIDS ini akan memberikan mekanisme deteksi dan pencegahan serangan dengan tingkat akurasi yang tinggi [2].

Dalam perancangan infrastruktur pemantauan tersebut, keamanan data investigasi dan rekam jejak digital forensik menjadi prioritas yang sama pentingnya dengan kapabilitas deteksi. Oleh karena itu, mesin Wazuh Manager ditempatkan secara Out-of-Band Logging di Disaster Recovery Center (DRC) yang terisolasi baik secara fisik maupun logis dari area produksi DMZ [10]. Praktik terbaik arsitektur pemusatan log yang terpisah ini bertujuan untuk memastikan bahwa seluruh data kejadian, rantai penjagaan, dan log ancaman tetap utuh serta keasliannya terjaga. Dengan penerapan arsitektur Out-of-Band ini, data bukti digital akan tetap aman dan tersedia untuk kepentingan analisis mendalam meskipun server di area DMZ sedang dieksploitasi, mengalami insiden pemadaman total (blackout), maupun terkena infeksi ransomware yang bersifat destruktif [11].

Tantangan besar yang menyertai implementasi SIEM pada jaringan skala besar adalah tingginya volume notifikasi peringatan yang tidak terstruktur, yang berpotensi memicu kelelahan analisis (alert fatigue) serta tingginya angka positif palsu (false positive) bagi tim administrator [12]. Untuk memitigasi isu tersebut, sangat esensial untuk memetakan log kejadian ke dalam kerangka kerja basis

pengetahuan global MITRE ATT&CK [13]. Standardisasi ini memfasilitasi administrator untuk mengklasifikasikan peringatan ancaman secara presisi ke dalam pola taktik dan teknik operasional penyerang, sehingga mitigasi dapat dilakukan secara strategis [14]. Keseluruhan rancang bangun arsitektur keamanan tingkat lanjut ini disusun menggunakan pendekatan metodologi siklus berkelanjutan Network Development Life Cycle (NDLC) yang meliputi tahap analisis, desain, simulasi purwarupa, implementasi, pemantauan, dan manajemen [15]. Berdasarkan seluruh argumentasi pemecahan masalah di atas, maka penelitian skripsi ini disusun dengan judul "IMPLEMENTASI SIEM BERBASIS WAZUH DAN SNORT IDS MENGGUNAKAN FRAMEWORK MITRE ATT&CK PADA JARINGAN DMZ".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada, rumusan masalah yang sesuai di dalam tugas akhir ini adalah:

1. Bagaimana merancang dan mengimplementasikan sistem *Security Information and Event Management* (SIEM) berbasis Wazuh dan Snort IDS menggunakan arsitektur *Out-of-Band Logging* pada lingkungan *Proof of Concept* (PoC)?
2. Bagaimana mengevaluasi sistem tersebut dalam mengekstraksi log dan mendeteksi serangan jaringan pada perangkat Ruckus ICX dan server Ubuntu, untuk kemudian dipetakan secara *real-time* ke dalam kerangka kerja MITRE ATT&CK?

1. 3 Batasan Masalah

Untuk menjaga agar ruang lingkup pembahasan lebih terarah dan dapat diselesaikan dalam waktu yang sudah ditentukan, maka tugas akhir ini memiliki batasan masalah sebagai berikut:

1. Rancang bangun dan implementasi sistem pemantauan keamanan difokuskan pada area jaringan *Demilitarized Zone* (DMZ) di Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) UIN Sunan Kalijaga. Penelitian ini tidak mencakup pemantauan di area jaringan internal kampus (*Campus Switch*) maupun area ekstranet lainnya.
2. Proses pengumpulan log kejadian (*event log*) perangkat keras hanya menarik data *raw log* dari perangkat *Core Switch* Ruckus ICX 7550-24F di DMZ menggunakan protokol rsyslog melalui port UDP 514. Sistem ini tidak mengumpulkan atau menganalisis log dari perangkat keamanan perimeter lain seperti *Next-Generation Firewall* (NGFW) atau *router gateway* ISP.
3. Arsitektur sistem SIEM tidak dirancang untuk *cluster* (*High Availability*). Wazuh Manager diimplementasikan beroperasi sebagai *Single Node All-in-One* (Manager, Dashboard, Filebeat, Indexer) di dalam lingkungan *Virtual Machine* (VM) *Server* yang ditempatkan secara *Out-of-Band* pada *Disaster Recovery Center* (DRC).
4. Wazuh Agent dan *Network Intrusion Detection System* (NIDS) Snort versi 3.12.1.0 diinstal secara bersamaan pada lingkungan VM Ubuntu di DRC, yang sekaligus difungsikan sebagai server web tiruan (*dummy web server*). Mengingat adanya restriksi *Promiscuous Mode* pada arsitektur virtualisasi *Production*, VM ini

difungsikan sebagai lingkungan simulasi (*Proof of Concept*) untuk mengawasi lalu lintas serangan yang mengarah ke sensor tersebut, bukan lalu lintas keseluruhan DMZ.

5. Sistem difungsikan murni untuk kegiatan pemantauan (*monitoring*), deteksi intrusi menggunakan Snort, serta manajemen peringatan dini (*alerting*) melalui Wazuh. Penelitian ini tidak menerapkan fitur pencegahan atau perbaikan otomatis (*Intrusion Prevention System / Active Response*), seperti pemblokiran alamat IP penyerang secara otomatis pada *firewall*.
6. Alur perancangan sistem dibatasi secara ketat menggunakan metode *Network Development Life Cycle* (NDLC) yang meliputi enam tahapan: *Analysis, Design, Simulation / Prototyping, Implementation, Monitoring, dan Management*.
7. Mesin penguji serangan (*attacker*) menggunakan sistem operasi Kali Linux. Skenario pengujian dibatasi pada pemetaan taktik *framework* MITRE ATT&CK dengan jenis simulasi meliputi: pemindaian jaringan (*Nmap/bash scripting*), eksploitasi kredensial (*Brute force* SSH pada Server Ubuntu dan *Switch* Ruckus & SNMP pada *Switch* Ruckus), serangan aplikasi web (*SQL Injection* dan *Cross-Site Scripting* pada *dummy web*), serta pengujian anomali volume paket (DoS).
8. Penelitian ini difokuskan pada perancangan, implementasi, dan evaluasi logika deteksi pada sistem SIEM (Wazuh dan Snort). Adapun penyediaan infrastruktur virtualisasi (*hypervisor*) serta konfigurasi lapisan inti (*core*) pada perangkat jaringan Ruckus ICX berada di luar cakupan penelitian dan merupakan wewenang penuh tim Network Engineer PTIPD UIN Sunan Kalijaga.

9. Penelitian ini difokuskan pada perancangan Proof of Concept (PoC) untuk menguji keberhasilan sistem dalam mendeteksi serangan nyata (True Positive) berdasarkan kerangka kerja MITRE ATT&CK. Proses optimasi tingkat lanjut, seperti tuning ruleset untuk mereduksi positif palsu (False Positive) atau manajemen noise pada log, berada di luar cakupan penelitian ini.
10. Penelitian ini tidak mencakup konfigurasi *hardening* keamanan tingkat lanjut pada antarmuka Wazuh Dashboard, seperti penerapan pembatasan akses alamat IP (*IP Whitelisting*). Mengingat adanya kebijakan *multi-zone network* pada lingkungan infrastruktur, antarmuka sistem berpotensi dapat diakses secara lebih luas tanpa restriksi zona jaringan yang ketat.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian tugas akhir ini dapat dijabarkan sebagai berikut:

1. Bagi Tim Engineer PTIPD

Penelitian ini memberikan manfaat praktis berupa efisiensi dalam proses pemantauan dan mitigasi ancaman siber. Ketersediaan platform SIEM yang terintegrasi memungkinkan tim *Network Operations Center* (NOC) atau *engineer* PTIPD untuk memvalidasi insiden keamanan secara akurat berbasis data log historis. Mekanisme peringatan dini (*alerting*) yang dipetakan menggunakan matriks MITRE ATT&CK juga akan membantu mempercepat waktu respons diagnosa masalah (*Mean Time to Detect*), sehingga stabilitas layanan dapat terus terjaga. Selain itu, purwarupa (*prototype*) sistem di lingkungan DRC ini dapat

menjadi landasan (*baseline*) teknis dan rekomendasi operasional bagi PTIPD untuk melakukan *deployment* agen SIEM secara menyeluruh ke *server* produksi DMZ di masa mendatang.

2. Bagi Akademisi

Penelitian ini diharapkan dapat menambah khazanah referensi kepustakaan bagi civitas akademika Program Studi Informatika. Secara khusus, penelitian ini dapat menjadi rujukan empiris terkait implementasi mekanisme pertahanan berlapis menggunakan integrasi *Host-based Intrusion Detection System* (HIDS), *Network Intrusion Detection System* (NIDS), dan pemanfaatan basis data intelijen ancaman (*Cyber Threat Intelligence*) dalam lingkungan infrastruktur jaringan skala perguruan tinggi.

3. Bagi Penulis

Penelitian ini berfungsi sebagai sarana untuk mengimplementasikan keilmuan yang telah dipelajari selama perkuliahan, khususnya pada konsentrasi rekayasa jaringan komputer. Selain itu, pengerjaan tugas akhir ini menjadi wadah pengembangan kompetensi dalam meningkatkan keahlian teknis (*hard skill*) terkait instalasi arsitektur sistem keamanan *open-source*, pembuatan *custom decoder* berbasis *Regular Expression* (Regex), serta pemahaman operasional mengenai pengujian intrusi dan kerentanan sistem.

1. 5 Tujuan Penelitian

Berdasarkan permasalahan yang di ajukan, tujuan dari pelaksanaan Capstone Design Project ini adalah:

1. Menerapkan tahapan metode *Network Development Life Cycle* (NDLC) secara sistematis dalam merancang dan membangun sistem *Security Information and Event Management* (SIEM) berbasis Wazuh dan Snort IDS versi 3 menggunakan arsitektur *Out-of-Band Logging* di area *Disaster Recovery Center* (DRC).
2. Membangun mekanisme sentralisasi pengumpulan log melalui konfigurasi *custom decoder* dan *correlation rules* untuk mengekstraksi *raw log* dari perangkat *Switch Ruckus ICX 7550-24F* di area DMZ, sekaligus menarik log lalu lintas ancaman dari lingkungan simulasi web server (*dummy web server*).
3. Mengevaluasi tingkat efektivitas sistem gabungan SIEM dan NIDS dalam mendeteksi skenario simulasi serangan spesifik (seperti *Port Scanning*, *Brute Force*, *DoS*, dan *Web Exploit*), serta memetakan peringatan dini (*alerts*) tersebut secara presisi ke dalam taktik dan teknik berdasarkan standar taksonomi global *framework* MITRE ATT&CK guna mengenali pola perilaku penyerang.

BAB V

PENUTUP

5. 1 Kesimpulan

Berdasarkan proses perancangan, implementasi, hingga pengujian sistem *Security Information and Event Management* (SIEM) terpusat pada infrastruktur jaringan PTIPD UIN Sunan Kalijaga, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Keberhasilan Implementasi Arsitektur *Out-of-Band Logging*

Sistem SIEM berbasis sumber terbuka menggunakan Wazuh dan sensor jaringan Snort 3 telah berhasil dirancang dan diimplementasikan. Penerapan arsitektur *Out-of-Band Logging* yang memadukan metode berbasis agen (*agent-based*) pada *server* Ubuntu dan nir-agen (*agentless*) menggunakan protokol Rsyslog pada perangkat *switch* Ruckus ICX terbukti efektif dalam memusatkan visibilitas keamanan, tanpa membebani kinerja utama pada infrastruktur produksi.

2. Efektivitas Kustomisasi Logika Deteksi

Untuk mendukung kemampuan sistem dalam mengekstraksi log mentah menjadi format terstruktur (JSON), modifikasi *Custom Decoder* berbasis ekspresi reguler (*Regex*) terbukti esensial dan berhasil membedah log dari infrastruktur *closed-system* (Ruckus) maupun sensor Snort. Selain itu, implementasi *Parent-Child Rule* mampu melakukan eskalasi tingkat keparahan peringatan secara dinamis berdasarkan frekuensi kejadian, sehingga sistem secara cerdas dapat membedakan anomali jaringan biasa dengan serangan bervolume tinggi seperti *Denial of Service* (DoS).

3. Evaluasi Deteksi Ancaman Berdasarkan MITRE ATT&CK

Hasil evaluasi kinerja sistem menunjukkan tingkat keberhasilan deteksi (*True Positive*) yang optimal secara *real-time*. Sistem secara akurat mampu mendeteksi dan memetakan seluruh skenario pengujian ke dalam kerangka kerja MITRE ATT&CK, yang mencakup taktik *Discovery* (T1046), *Credential Access* (T1110), *Initial Access* (T1189 & T1190), serta *Impact* (T1498). Keseluruhan deteksi tersebut divisualisasikan secara komprehensif dengan metrik latensi yang sangat responsif, memberikan visibilitas forensik utuh bagi administrator keamanan.

5. 2 Saran

Mengingat adanya batasan masalah dalam penelitian ini serta potensi perkembangan teknologi di masa depan, penulis mengajukan beberapa saran untuk pengembangan sistem selanjutnya:

1. Optimasi Positif Palsu (False Positive Tuning):

Penelitian selanjutnya disarankan untuk melakukan proses *tuning* dan kalibrasi tingkat lanjut pada *ruleset* sistem. Hal ini bertujuan untuk menekan angka peringatan yang tidak relevan (positif palsu) dan mereduksi kelelahan analisis (*alert fatigue*), sehingga sistem dapat lebih fokus pada ancaman yang benar-benar esensial di lingkungan produksi.

2. Implementasi Mekanisme Active Response:

Sistem yang dibangun pada *Proof of Concept* (PoC) ini masih berfokus pada pemantauan dan deteksi intrusi (IDS). Pengembangan ke depan dapat memaksimalkan fitur *Active Response* pada Wazuh Manager untuk menjadikannya sistem pencegahan (IPS), di mana sistem dapat secara otomatis

merespons ancaman, misalnya dengan memblokir alamat IP penyerang melalui dinding api (*firewall*) ketika eskalasi Level 15 terpicu.

3. Integrasi dengan Threat Intelligence:

Untuk meningkatkan akurasi deteksi ancaman tingkat lanjut, disarankan untuk mengintegrasikan SIEM dengan platform *Threat Intelligence* pihak ketiga, seperti MISP (*Malware Information Sharing Platform*), AlienVault OTX, atau VirusTotal. Integrasi ini akan memperkaya basis data *ruleset* dengan indikator kompromi (IoC) terbaru yang diperbarui secara global.

4. Penerapan Arsitektur High Availability (Clustering):

Guna mengantisipasi lonjakan volume log jaringan yang masif pada saat sistem diimplementasikan secara penuh di seluruh lingkungan PTIPD, penelitian selanjutnya dapat menerapkan arsitektur *Wazuh Cluster* dan *Load Balancer*. Pendekatan ini akan menjamin ketersediaan sistem yang tinggi (*High Availability*) dan mencegah terjadinya kelebihan beban (*overload*) pada satu *server* pusat.

5. Pengadaan Sensor NIDS Fisik Terdedikasi (Dedicated Hardware):

Mengingat adanya restriksi kebijakan keamanan pada infrastruktur virtualisasi kampus (VMware vSphere) yang menolak penerapan mode *Promiscuous*, cakupan pemantauan sensor NIDS virtual saat ini menjadi terbatas. Untuk pengembangan selanjutnya, apabila institusi ingin melakukan pemindaian lalu lintas (*sniffing*) secara menyeluruh terhadap seluruh server di lingkungan DMZ maupun fasilitas DRC, disarankan untuk menggunakan perangkat keras sensor fisik

tersendiri. Sensor fisik tersebut dapat diintegrasikan memanfaatkan fitur SPAN (*Switched Port Analyzer*) atau *Port Mirroring* langsung dari *core switch* produksi (Ruckus ICX), sehingga seluruh lalu lintas jaringan dapat direplikasi dan dianalisis tanpa terhalang oleh batasan *virtual switch*.



DAFTAR PUSTAKA

- [1] I. Alqasam, “Implementasi Keamanan Berbasis SIEM (Security Information and Event Management) Menggunakan QRadar Sebagai Pendeteksi Ancaman Keamanan Siber,” pp. 1–55, 2024.
- [2] M. R. Reza Pahlevi, C. Umam, and L. B. Handoko, “Deteksi dan Pencegahan Web Defacing Judi Online dengan Wazuh SIEM dan Snort IDS Berbasis Signature,” *Jurnal Algoritma*, vol. 22, no. 1, pp. 197–208, 2025, doi: 10.33364/algoritma/v.22-1.2220.
- [3] J. Myllylä, “Detecting Cyber Attacks in Time-Combining Attack Simulation With Detection Logic,” 2021.
- [4] T. Lee, “a Comprehensive Analysis of Challenges and Strategies in Enhancing Cyber Security for the Defense Industry,” vol. 5, no. 1, pp. 70–80, 2024.
- [5] MoE, *Digital education strategy and implementation plan 2023 -2028*, vol. 1, no. 1. 2023.
- [6] R. Hasan, “Safeguarding of Financial Organization from Cyber-Attack using Next Generation Firewall (NGFW), Security Information & Event Management (SIEM) and Honeypot,” *Dublin Business School*, no. January, pp. 1–132, 2024, [Online]. Available: <https://hdl.handle.net/10788/4501>
- [7] “Snort 3 Inspector Reference - Introduction [Cisco Secure Firewall Management Center] - Cisco.” Accessed: May 07, 2026. [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference/intro.html>
- [8] A. Kamil, M. Tahir, S. Julia, M. Misfarah, A. Laviva Rahmat, and Y. Dwi Mahendra, “Sistem Keamanan Berbasis Host-Based Intrusion Detection System (Hids) Menggunakan

- Wazuh,” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 3, pp. 5460–5466, 2025, doi: 10.36040/jati.v9i3.14267.
- [9] F. Arman *et al.*, “IMPLEMENTASI MONITORING DAN PENCEGAHAN SERANGAN DEFACEMENT JUDI ONLINE MENGGUNAKAN WAZUH,” vol. 10, no. 1, pp. 1309–1317, 2026.
- [10] K. Sicard, “The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks,” *The Kennesaw Journal of Undergraduate Research*, vol. 6, no. 2, 2019, doi: 10.62915/2474-4921.1167.
- [11] “5 Tips Efektif Mencegah DRC (Disaster Recovery Center).” Accessed: May 07, 2026. [Online]. Available: <https://www.domainesia.com/tips/drc/>
- [12] A. Z. A. Adrian, R. A. Megantara, and F. Al Zami, “Hybrid Multilayer Architecture Integrating Suricata, Wazuh, and Cyber Threat Intelligence for Drive-by-Download Malvertising Detection,” *Sinkron*, vol. 10, no. 1, pp. 161–168, 2026, doi: 10.33395/sinkron.v10i1.15616.
- [13] B. Al-Sada, A. Sadighian, and G. Oligeri, “Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database,” *IEEE Access*, vol. 12, no. December 2023, pp. 1217–1234, 2024, doi: 10.1109/ACCESS.2023.3344680.
- [14] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing mitre att&ck risk using a cyber-security culture framework,” *Sensors*, vol. 21, no. 9, 2021, doi: 10.3390/s21093267.
- [15] Miftahur Rahman, Ravi Budi Handwika, and Ahadini Izzatus Zahro, “Penerapan Model Network Development Life Cycle (NDLC) Pada Infrastruktur Jaringan Internet Kantor Desa Kemiri,” *Jurnal Publikasi Teknik Informatika*, vol. 2, no. 3, pp. 37–47, 2023, doi: 10.55606/jupti.v2i3.1790.

- [16] Z. E. Nurmi Hidayasari, Mansur, Kasmawi, “Implementasi Prototipe SIEM Berbasis Wazuh pada Website dengan Pengujian FIM dan Threat Hunting,” vol. 6, no. 4, pp. 372–382, 2025, doi: 10.62527/jitsi.
- [17] D. E. Journal, “Siber Güvenlik ve Dijital Ekonomi Dergisi Cybersecurity and Digital Economy Journal Design and Implementation of a Network Intrusion Detection System Using Snort 3 in a Virtualized Linux Environment Aly Abdelhalima , a *,” vol. 1, no. 2, pp. 111–119, 2025.
- [18] K. M. Muhammad Alvan Ekawan Putra, I Putu Hariyadi, “OTOMATISASI KONFIGURASI WAZUH TERINTEGRASI VIRUSTOTAL MENGGUNAKAN ANSIBLE UNTUK MENDETEKSI DAN MEMPROTEKSI SERANGAN MALWARE,” vol. 11, no. 1, pp. 55–66, 2025.
- [19] “What Is a Demilitarized Zone (DMZ) in Network Security and How Does It Work? | by Cyberpro Magazine | Medium.” Accessed: May 07, 2026. [Online]. Available: <https://medium.com/@cyberpromagazine/what-is-a-demilitarized-zone-dmz-in-network-security-and-how-does-it-work-480213260a7b>
- [20] “Techniques - Enterprise | MITRE ATT&CK®.” Accessed: May 07, 2026. [Online]. Available: <https://attack.mitre.org/techniques/enterprise/>
- [21] “Memantau perangkat jaringan dengan Wazuh | Wazuh.” Accessed: May 07, 2026. [Online]. Available: <https://wazuh.com/blog/monitoring-network-devices/>
- [22] “Rocky Linux Vs Ubuntu: Features, Pros & Ideal Use Cases.” Accessed: May 07, 2026. [Online]. Available: <https://tuxcare.com/blog/rocky-linux-vs-ubuntu/>
- [23] “View of Information Security Systems Design Using SIEM, SOAR and Honeypot.” Accessed: May 16, 2026. [Online].

Available:

<https://jptam.org/index.php/jptam/article/view/4850/4124>

- [24] “How to set a cron job to run a shell script? - Ask Ubuntu.” Accessed: May 16, 2026. [Online]. Available: <https://askubuntu.com/questions/350861/how-to-set-a-cron-job-to-run-a-shell-script>
- [25] “Custom decoders - Decoders · Wazuh documentation.” Accessed: May 16, 2026. [Online]. Available: <https://documentation.wazuh.com/current/user-manual/ruleset/decoders/custom.html>
- [26] “Custom rules - Rules · Wazuh documentation.” Accessed: May 16, 2026. [Online]. Available: <https://documentation.wazuh.com/current/user-manual/ruleset/rules/custom.html>

