

**RANCANG BANGUN DAN EVALUASI EFEKTIVITAS SURICATA
DENGAN GRAFANA PADA *DATA CENTER* INTERNAL PTIPD**

TUGAS AKHIR

Untuk memenuhi sebagian persyaratan

Mencapai derajat Sarjana S-1

Program Studi Informatika



Disusun Oleh :

Mochammad Cah Anugrah Gusti

NIM.22106050006

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

2026

HALAMAN 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-2109/Un.02/DST/PP.00.9/08/2026

Tugas Akhir dengan judul : RANCANG BANGUN DAN EVALUASI EFEKTIVITAS SURICATA DENGAN GRAFANA PADA DATA CENTER INTERNAL PTIPD

yang dipersiapkan dan disusun oleh:

Nama : MOCHAMMAD CAH ANUGRAH GUSTI
Nomor Induk Mahasiswa : 22106050006
Telah diujikan pada : Kamis, 13 Agustus 2026
Nilai ujian Tugas Akhir : A-

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

TIM UJIAN TUGAS AKHIR



Valid ID: 6a86dbc6082ad

Ketua Sidang

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



Valid ID: 6a86b2de64e27

Penguji I

Dr. Agung Fatwanto, S.Si., M.Kom.
SIGNED



Valid ID: 6a86b379f336c

Penguji II

Dr. Ir. Sumarsono, S.T., M.Kom.
SIGNED



Valid ID: 6a86ef826a585

Yogyakarta, 13 Agustus 2026
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi
Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

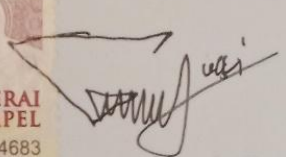
Yang bertanda tangan dibawah ini:

Nama : Mochammad Cah Anugrah Gusti
NIM : 22106050006
Program Studi : Informatika
Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya, bahwa skripsi saya yang berjudul **Rancang Bangun dan Evaluasi Efektivitas Suricata dengan Grafana pada Data Center Internal PTIPD** 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, 30 Juli 2026




Mochammad Cah Anugrah Gusti
22106050006

LEMBAR PERSETUJUAN TUGAS AKHIR



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 : Mochammad Cah Anugrah Gusti

NIM : 22106050006

Judul Skripsi : Rancang Bangun dan Evaluasi Efektivitas Suricata dengan Grafana pada Data Center Internal PTIPD

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.

Yogyakarta, 30 Juli 2026

Pembimbing

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

NIP. 19751024 200912 1 002

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, Dokumen ini diperkenankan dipakai sebagai referensi kepastakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen tugas akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.



ABSTRAK

Infrastruktur jaringan Data Center Internal PTIPD UIN Sunan Kalijaga menghadapi celah keamanan (*blindspot*) pada lapisan aplikasi (Layer 7) akibat keterbatasan *Deep Packet Inspection* (DPI) pada *Edge Firewall* komersial, serta minimnya visibilitas terhadap pergerakan lateral (*Lateral Movement*) antar segmen VLAN internal (*East-West Traffic*). Penelitian ini merancang dan mengimplementasikan sistem *Intrusion Detection System* (IDS) berbasis Suricata yang terintegrasi dengan ekosistem observabilitas *PLG Stack* (*Promtail, Loki, Grafana*) menggunakan arsitektur *Staged Deployment* dua *Virtual Machine*. Metodologi penelitian mengintegrasikan *Network Development Life Cycle* (NDLC) sebagai kerangka pengembangan, *Penetration Testing Execution Standard* (PTES) sebagai standar pengujian, dan *Framework* MITRE ATT&CK sebagai taksonomi skenario serangan. Simulasi *Inter-VLAN Lateral Movement* dilaksanakan pada lingkungan terisolasi *Docker Bridge Network*, sementara pemantauan trafik nyata dilakukan melalui *interface* ENS yang membaca *syslog* *Core Campus Switch*. Efektivitas sistem dievaluasi menggunakan *Confusion Matrix* terhadap 17 titik data dari empat hari pengujian. Hasil evaluasi pada skenario pengujian terkontrol menunjukkan nilai *Precision*, *Recall*, dan *Accuracy* masing-masing sebesar 100% dari 16 sesi *True Positive* tanpa *False Positive* maupun *False Negative*. *Custom Rules* yang dikembangkan berkontribusi pada 62,5% total deteksi, termasuk deteksi eksklusif pola *Lateral Movement* yang tidak tercakup *ruleset* publik.

Kata Kunci: Suricata, *PLG Stack*, MITRE ATT&CK, *Lateral Movement*, *Custom Rules*



ABSTRACT

PTIPD UIN Sunan Kalijaga network faces application-layer (Layer 7) security blindspots due to limited Deep Packet Inspection (DPI) on commercial edge firewalls and a lack of visibility into Inter-VLAN lateral movement (East-West traffic). This study designs and implements a Suricata-based Intrusion Detection System (IDS) integrated with a resource-efficient Promtail, Loki, and Grafana (PLG) observability stack using a staged two-Virtual Machine architecture. The methodology integrates the Network Development Life Cycle (NDLC), the Penetration Testing Execution Standard (PTES), and the MITRE ATT&CK framework. Simulations were executed in an isolated Docker Bridge Network, while real-world traffic was monitored via the ENS interface reading Core Switch syslog. System effectiveness was evaluated using a Confusion Matrix against 17 data points over four testing days. Controlled testing demonstrated 100% Precision, Recall, and Accuracy across 16 True Positive sessions, with zero False Positives or False Negatives. The developed Custom Rules contributed to 62.5% of total detections, enabling exclusive detection of lateral movement patterns uncovered by public rulesets.

Keywords: *Suricata, PLG Stack, MITRE ATT&CK, Lateral Movement, Custom Rules*



MOTTO

Seseorang tidak akan mendapatkan apa-apa kecuali apa yang telah ia usahakan dengan sungguh-sungguh

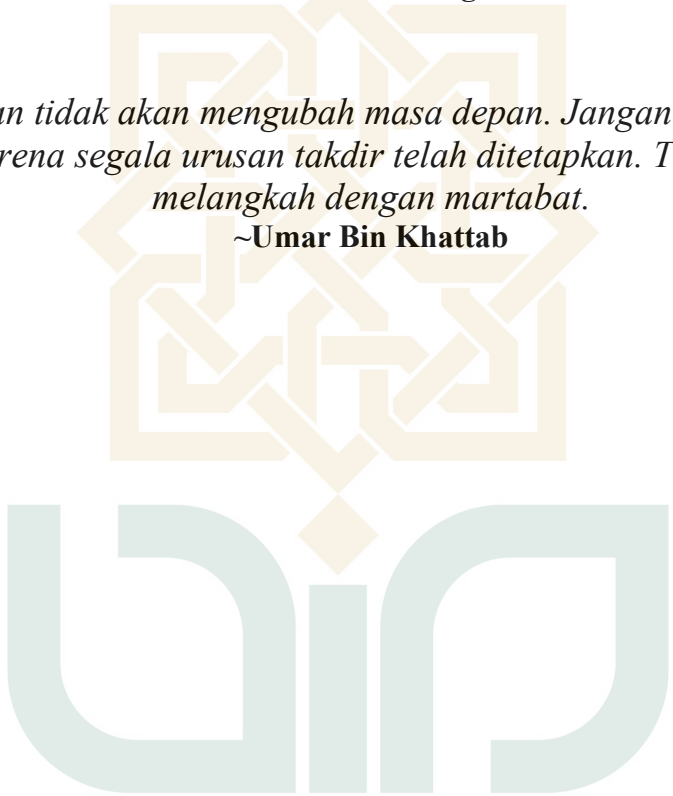
~Xiaoyan

Orang-orang pintar selalu memfokuskan diri pada hal-hal yang benar-benar penting.

~Jensen Huang

Kekhawatiran tidak akan mengubah masa depan. Jangan menyiksa dirimu sendiri, karena segala urusan takdir telah ditetapkan. Tugasmu adalah melangkah dengan martabat.

~Umar Bin Khattab



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

HALAMAN PERSEMBAHAN

Atas kehendak dan karunia Allah SWT, skripsi ini penulis persembahkan kepada:

Allah SWT, yang telah memberikan kekuatan, kesabaran, petunjuk, dan kemudahan dalam menyelesaikan setiap tahapan perjalanan ini

Kedua Orang Tua Penulis, Mochammad Suchayonoto dan Ibu Lilik Handayani, atas doa yang tiada henti, kasih sayang, serta dukungan moral dan material yang menjadi landasan utama perjuangan penulis.

Untuk penulis untuk diri sendiri, terima kasih telah bertahan, terus melangkah, dan tidak menyerah meskipun perjalanan ini tidak selalu mudah untuk dilalui. Terima kasih atas segala kerja keras hingga mampu sampai pada titik ini.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Dan

Almamater Tercinta,

Program Studi Informatika
Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ وَالصَّلَاةُ وَالسَّلَامُ عَلَى سَيِّدِنَا مُحَمَّدٍ وَعَلَى آلِهِ وَصَحْبِهِ أَجْمَعِينَ

اللَّهُمَّ ارْزُقْنَا فَهْمَ النَّبِيِّينَ وَحِفْظَ الْمُرْسَلِينَ وَإِلْهَامَ الْمَلَائِكَةِ الْمُقَرَّبِينَ، وَارْحَمْنَا بِرَحْمَتِكَ يَا أَرْحَمَ الرَّاحِمِينَ،

أَمِينَ

Alhamdulillah rabbil'alam, tiada puji dan syukur yang pantas terucap selain kepada Allah SWT, Sang Pemilik Semesta Alam, atas segala limpahan rahmat, iradah, dan karunia-Nya. Hanya dengan rida dan izin-Nya, penyusunan tugas akhir yang berjudul **“Rancang Bangun dan Analisis Efektivitas Suricata dengan Grafana pada Data Center Internal PTIPD”** ini dapat diselesaikan dengan baik. Shalawat serta salam senantiasa tercurahkan kepada teladan abadi kita, Nabi Muhammad SAW, yang syafaatnya senantiasa dinantikan kelak di hari akhir.

Tugas akhir ini disusun sebagai salah satu syarat mutlak untuk meraih gelar Sarjana Komputer (S.Kom.) pada Program Studi Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga Yogyakarta. Penulis menyadari sepenuhnya bahwa karya ini lahir dari keterbatasan ilmu dan pengalaman yang penulis miliki. Oleh karena itu, dengan segala kerendahan hati, penulis sangat menantikan kritik, saran, serta nasihat yang membangun demi penyempurnaan karya ini.

Sebuah perjalanan panjang tidak akan pernah sampai pada tujuannya tanpa uluran tangan dari orang lain. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sedalam-dalamnya kepada:

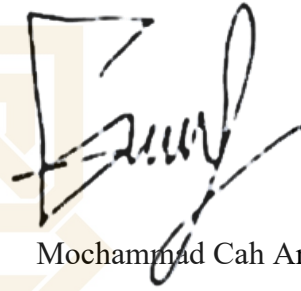
1. Kedua Orang Tua Tercinta, Mochammad Suchayonoto dan Ibu Lilik Handayani, yang selalu memberikan doa, dukungan moral, fasilitas, serta motivasi tiada henti dalam setiap langkah kehidupan penulis.
2. Bapak Prof. Noorhaidi Hasan, S.Ag., M.A., M.Phil., Ph.D. selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si. selaku Dekan Fakultas Sains dan Teknologi.
4. Bapak Dr. Muhammad Mustakim, S.T., M.T. selaku Ketua Program Studi Informatika.
5. Bapak Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng selaku Dosen Pembimbing Tugas Akhir, yang dengan penuh kesabaran dan ketulusan memberikan bimbingan, arahan, saran, serta masukan berharga hingga karya ini selesai.
6. Bapak Dr. Agus Mulyanto, S.Si., M.Kom., ASEAN Eng. selaku Dosen Penasihat Akademik, yang telah memberikan pengarahan dan bimbingan akademik selama masa studi.
7. Kepala dan Seluruh Staf PTIPD UIN Sunan Kalijaga Yogyakarta, yang telah memberikan izin, akses, serta bantuan teknis selama pelaksanaan penelitian pada infrastruktur Data Center.
8. Seluruh Dosen dan Karyawan Program Studi Informatika UIN Sunan Kalijaga Yogyakarta, yang telah membagikan ilmu, pengalaman, serta pelayanan administrasi selama masa pendidikan.
9. Rekan-rekan Mahasiswa Informatika, khususnya angkatan 2022, yang menjadi teman seperjuangan dalam berdiskusi, berbagi ilmu, dan menghadapi tantangan akademik bersama.
10. Rekan-rekan Beasiswa Djarum, khususnya angkatan 2024/2025, yang menjadi teman seperjuangan dalam berdiskusi, berbagi ilmu, dan menghadapi tantangan akademik bersama.
11. Masa Kopi dan Sebelas Coffee, yang menjadi salah satu tempat favorit penulis untuk menyelesaikan berbagai bagian tugas akhir ini, sekaligus tempat untuk menenangkan pikiran dan mengembalikan semangat selama proses penyusunan karya ini.
12. Terima kasih untuk diri sendiri yang telah mampu bertahan dan terus melangkah hingga sampai pada titik ini. Terima kasih karena tidak memilih menyerah meskipun harus menghadapi berbagai tantangan dan proses panjang selama penyusunan tugas

akhir ini. Semoga seluruh proses yang telah dilalui menjadi awal dari langkah-langkah baik ke depannya.

Penulis berharap semoga Allah SWT membalas seluruh kebaikan dan bantuan yang telah diberikan oleh berbagai pihak. Semoga tugas akhir ini memberikan manfaat akademis maupun praktis bagi pengembangan ilmu pengetahuan. Aamiin.

Yogyakarta, 11 Agustus 2026

Penulis,



Mochammad Cah Anugrah Gusti



STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR ISI

HALAMAN PENGESAHAN	ii
LEMBAR PERNYATAAN KEASLIAN.....	iii
LEMBAR PERSETUJUAN TUGAS AKHIR	iv
LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR	v
ABSTRAK.....	vi
ABSTRACT	vii
MOTTO	viii
HALAMAN PERSEMBAHAN	ix
KATA PENGANTAR	x
DAFTAR ISI.....	xiii
DAFTAR TABEL.....	xvii
DAFTAR GAMBAR.....	xviii
DAFTAR LAMPIRAN.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
1.5.1 Bagi Institusi (UPT PTIPD UIN Sunan Kalijaga)	5
1.5.2 Bagi Ilmu Pengetahuan dan Akademik.....	5
1.5.3 Bagi Peneliti.....	5
BAB II KAJIAN PUSTAKA.....	7
2.1 Tinjauan Pustaka.....	7
Posisi Penelitian (<i>State of the art</i>).....	10
2.2 Keamanan Jaringan Data Center.....	11
2.2.1 Paradigma Assume Breach	11
2.2.2 East-West Traffic dan Inter-VLAN <i>Lateral Movement</i>	12
2.2.3 Mekanisme Inspeksi dengan Mode AF-Packet.....	12
2.3 <i>Framework</i> MITRE ATT&CK.....	12
2.4 Sistem Deteksi Intrusi (IDS).....	13
2.4.1 Suricata dan Deep Packet Inspection (DPI) Layer 7	13

2.4.2 Custom Rules Suricata.....	14
2.5 Standar Pengujian Keamanan (PTES)	14
2.6 Ekosistem Observabilitas PLG Stack	15
2.7 Virtualisasi dan Virtual Machine	16
2.7.1 Kontainerisasi dan Docker Bridge Network	16
2.8 Network Development Life Cycle (NDLC)	17
2.9 Evaluasi Performa dengan Confusion Matrix.....	18
2.9.1 Unit Analisis Per Sesi Serangan	19
2.9.2 Parameter Evaluasi.....	19
BAB III METODE PENGEMBANGAN SISTEM.....	20
3.1 Jenis Penelitian.....	20
3.2 Waktu dan Tempat Penelitian	20
3.3 Alur Penelitian	21
3.4 Alat dan Bahan Penelitian.....	22
3.4.1 Perangkat Keras (Hardware).....	22
3.4.2 Perangkat Lunak (Software)	23
3.5 Tahap Analysis (Analisis).....	24
3.5.1 Identifikasi Topologi dan Infrastruktur PTIPD.....	24
3.5.2 Identifikasi Celah Keamanan (<i>Blindspot</i>).....	24
3.5.3 Analisis Kebutuhan Sistem	26
3.6 Tahap Design (Desain)	26
3.6.1 Desain Arsitektur Dua Virtual Machine	26
3.6.2 Desain Topologi Jaringan Simulasi Docker	27
3.6.3 Desain <i>Pipeline</i> Observabilitas PLG	28
3.6.4 Desain Custom Rules Suricata.....	29
3.7 Metodologi Pengujian Keamanan (PTES).....	29
3.7.1 Fase yang Digunakan.....	29
3.7.2 Fase yang Tidak Digunakan.....	30
3.8 Tahap Simulation (Simulasi)	31
3.8.1 Aktivitas Simulasi di Lab PJK.....	31
3.8.2 Implementasi Custom Rules Suricata	32
3.8.3 Kriteria Keberhasilan Simulasi	32
3.9 Tahap Implementation (Implementasi).....	32
3.9.1 Replikasi Konfigurasi ke VM PTIPD	33
3.9.2 Tuning Ruleset Menggunakan Log <i>Real-time</i> PTIPD	33
3.10 Tahap <i>Monitoring</i> (Pemantauan) Pelaksanaan Skenario Pengujian	34
3.10.1 Perancangan Skenario Serangan Berbasis MITRE ATT&CK	34

3.10.2 Empat Kondisi Pengujian	35
3.10.3 Prosedur Pengumpulan Data.....	36
3.11 Tahap Management (Pengelolaan) Analisis Data.....	36
3.11.1 Kalkulasi Confusion Matrix.....	37
3.11.2 Perhitungan Parameter Evaluasi	38
3.11.3 Kriteria Kelayakan Sistem	38
3.12 Ringkasan Integrasi Metodologi.....	39
BAB IV PERANCANGAN DAN EVALUASI SISTEM	40
4.1 Hasil Tahap Analysis	40
4.1.1 Topologi Infrastruktur PTIPD Eksisting.....	40
4.1.2 Identifikasi <i>Blindspot</i> Keamanan Layer 7.....	41
4.1.3 Rekapitulasi Kebutuhan Sistem	46
4.2 Hasil Tahap Design.....	48
4.2.1 Arsitektur Dua Virtual Machine	49
4.2.2 Topologi Jaringan Simulasi Docker.....	51
4.2.3 <i>Pipeline</i> Observabilitas PLG Stack.....	52
4.2.4 Desain Custom Rules Suricata.....	53
4.2.5 Rancangan Skenario Serangan.....	55
4.3 Hasil Tahap Simulation Validasi di Lab PJK	57
4.3.1 Hasil Konfigurasi Sistem di Lab PJK	57
4.3.2 Hasil Pengujian Custom Rules.....	59
4.3.3 Hasil Validasi <i>Pipeline</i> PLG.....	60
4.3.4 Hasil Verifikasi Kriteria Keberhasilan Simulasi.....	61
4.4 Hasil Tahap Implementation Replikasi ke Data Center PTIPD.....	62
4.4.1 Hasil Konfigurasi Sistem di PTIPD	63
4.4.2 Hasil Verifikasi Custom Rules di PTIPD	64
4.4.3 Hasil Verifikasi <i>Pipeline</i> PLG di PTIPD	65
4.4.4 Hasil Verifikasi Interface ENS Pembacaan Trafik Core Switch PTIPD	68
4.4.5 Hasil Verifikasi Kriteria Keberhasilan Implementation	69
4.5 Hasil Tahap <i>Monitoring</i>	70
4.5.1 Kondisi Tenang Sesi 1 Jam Kerja (Hari 1)	71
4.5.2 Kondisi Serang Sesi 1 Fase Eksternal (Hari 2).....	73
4.5.3 Kondisi Serang Sesi 2 Fase Internal (Hari 3).....	75
4.5.4 Kondisi Bersamaan Stress Time (Hari 4)	77
4.5.5 Rekapitulasi Hasil <i>Monitoring</i>	83
4.6 Hasil Tahap Management	84
4.6.1 Kalkulasi Parameter Evaluasi	84

4.6.2 Analisis Hasil Evaluasi	85
4.6.3 Perbandingan Deteksi ET Open vs Custom Rules.....	88
4.6.4 Rekomendasi Arsitektur Keamanan	89
4.6.5 Keterbatasan Penelitian.....	90
BAB V PENUTUP	92
5.1 Kesimpulan	92
5.2 Saran	93
DAFTAR PUSTAKA	94



DAFTAR TABEL

Tabel 4.1 Identifikasi <i>Blindspot</i> Keamanan pada Infrastruktur PTIPD	44
Tabel 4.2 Data Kuantitatif Ancaman dari <i>Dashboard</i> Cisco FMC.	45
Tabel 4.3 Rekapitulasi Kebutuhan Fungsional dan Solusi yang Dirancang.....	47
Tabel 4.4 Scope dan Rules of Engagement Pengujian (PTES Phase 1)	49
Tabel 4.5 Anatomi Custom Rules Suricata untuk Inter-Subnet <i>Lateral Movement</i>	54
Tabel 4.6 Rancangan Final Skenario Serangan Berbasis MITRE ATT&CK.....	56
Tabel 4.7 Hasil Verifikasi Kriteria Keberhasilan Simulasi	61
Tabel 4.8 Perbandingan Spesifikasi Lingkungan Lab PJK vs Data Center PTIPD.....	62
Tabel 4.9 Hasil Verifikasi Kriteria Keberhasilan Implementation	69
Tabel 4.10 Hasil <i>Monitoring</i> Kondisi Tenang (Hari 1)	72
Tabel 4.11 Hasil Monitoring Kondisi Serang Sesi 1 Fase Eksternal (Hari 2)	75
Tabel 4.12 Hasil <i>Monitoring</i> Kondisi Serang Sesi 2 Fase Internal (Hari 3).....	77
Tabel 4.13 Hasil <i>Monitoring</i> Kondisi Bersamaan Stress Time (Hari 4).....	82
Tabel 4.14 Rekapitulasi Confusion Matrix per Kondisi Pengujian	83
Tabel 4.15 Rekapitulasi Confusion Matrix Keseluruhan.....	83
Tabel 4.16 Hasil Kalkulasi Parameter Evaluasi Confusion Matrix	84
Tabel 4.17 Distribusi Deteksi per Sumber Ruleset (Berdasarkan Sesi).....	88

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Matriks Confusion Matrix dan Parameter Evaluasi	19
Gambar 3.1 Alur Penelitian Berbasis NDLC.....	22
Gambar 3.2 Topologi Jaringan Data Center PTIPD	24
Gambar 3.3 Arsitektur Holistik Jaringan, Posisi Pengguna, dan Blindspot Berdasarkan Model OSI.....	25
Gambar 3.4 Arsitektur Dua Virtual Machine	27
Gambar 3.5 Topologi Jaringan Simulasi Docker Bridge Network.....	28
Gambar 3.6 Diagram Alur Pipeline PLG Stack.....	28
Gambar 3.7 Validasi Sistem pada Tahap Simulasi di Lab PJK.....	31
Gambar 3.8 Sistem Berhasil Diimplementasikan di VM PTIPD	33
Gambar 3.9 Visualisasi Confusion Matrix dan Rumus Evaluasi.....	38
Gambar 4.1 Topologi Jaringan Ekisting Data Center PTIPD UIN Sunan Kalijaga	41
Gambar 4. 2 Dashboard Cisco FMC Keseluruhan Intrusion Events dalam 1 Hari	42
Gambar 4.3 <i>Dashboard</i> Cisco FMC Total Events Berdasarkan Protokol Aplikasi	42
Gambar 4.4 <i>Dashboard</i> Cisco FMC Indikasi Kompromi pada Host Internal	43
Gambar 4.5 <i>Dashboard</i> Cisco FMC Detail Events SERVER-MYSQL Authentication Bypass	43
Gambar 4.6 Arsitektur Dua Virtual Machine	50
Gambar 4. 7 Topologi Jaringan Simulasi Docker Bridge Network.....	52
Gambar 4. 8 Diagram Alur <i>Pipeline</i> PLG Stack.....	53
Gambar 4.9 Kode Custom Rules Suricata untuk Inter-VLAN <i>Lateral Movement</i>	55
Gambar 4.10 Suricata v8.0.4 Berjalan dengan Status Active di VM-Engine Lab PJK.....	58
Gambar 4.11 Topologi Docker Bridge Network dengan Tiga Kontainer Aktif di Lab PJK.....	59
Gambar 4.12 Alert Custom Rules SID 9001001–9007003 Pertama Kali Terdeteksi di eve.json Lab PJK	60
Gambar 4.13 <i>Dashboard</i> Grafana Menampilkan Data Alert dari Lab PJK secara <i>Real-time</i>	61
Gambar 4.14 Suricata v8.0.4 Berjalan dengan Status Active di VM-Engine PTIPD.....	63
Gambar 4.15 Topologi Docker Bridge Network Terbentuk dengan Tiga Kontainer Aktif di PTIPD	64
Gambar 4. 16 Custom Rules SID 9001001–9007003 Aktif dan Terverifikasi di Lingkungan PTIPD	65

Gambar 4. 17 Tampilan Utama <i>Dashboard Monitoring</i> Suricata dengan Struktur Navigasi Tab	67
Gambar 4.18 Tampilan Utama <i>Dashboard Monitoring</i> Suricata dengan Struktur Navigasi Tab	69
Gambar 4.19 Overview Dashboard Hari 1	71
Gambar 4. 20 Pola Waktu Aktivitas Alert	72
Gambar 4. 21 Tren Alert per Tingkat Bahaya Hari 1	72
Gambar 4. 22 Screenshot Grafana <i>dashboard</i> saat Skenario 1 (Nmap) dieksekusi tampilkan panel Pola Waktu dengan lonjakan alert pada timestamp 15:00–15:50 WIB. ...	74
Gambar 4. 23 Screenshot eve.json menampilkan alert dengan field `alert.signature` berisi ET SCAN Nmap dan field `iface` berisi nama Docker Bridge interface.	74
Gambar 4. 24 Screenshot Grafana saat Skenario 2 (Hydra) tampilkan alert Custom pada panel Realtime Alerts.....	74
Gambar 4. 25 Screenshot Grafana saat Skenario 3 (SSH <i>Lateral Movement</i>) tampilkan alert Custom sebagai bukti empiris novelty custom rules.	74
Gambar 4. 26 Screenshot Grafana saat Skenario 4 (Nmap Internal) tampilkan alert Custom pada panel Top 10 Aturan Paling Sering Terpucu dari Mitre Attack.	76
Gambar 4. 27 Screenshot Grafana saat Skenario 5 (SQLmap) tampilkan lonjakan 40 alert ET EXPLOIT SQL Injection pada panel Pola Waktu Aktivitas Alert.	76
Gambar 4. 28 Screenshot Grafana saat Skenario 6 (curl Path Traversal) tampilkan alert ET WEB_SERVER Path Traversal pada panel Realtime Alerts.....	76
Gambar 4.29 Grafana saat Skenario 7 (hping3) tampilkan alert ET DOS pada panel Pola Waktu Aktivitas Alert dengan pola lonjakan trafik DoS.	76
Gambar 4. 30 Ringkasan Eksekutif <i>Dashboard Monitoring</i> Suricata pada Kondisi Bersamaan Hari 4.....	78
Gambar 4. 31 Pola Waktu Aktivitas Alert Selama Kondisi Bersamaan Hari 4.....	79
Gambar 4.32 Rasio Distribusi Alert per Interface pada Kondisi Bersamaan Hari 4	79
Gambar 4.33 Aktivitas Serangan per Tingkat Bahaya pada Kondisi Bersamaan Hari 4	80
Gambar 4.34 Distribusi Rules Paling Sering Terpucu pada Kondisi Bersamaan Hari 4.....	80
Gambar 4.35 Detail Forensik Realtime Alert pada Kondisi Bersamaan Hari 4	81
Gambar 4. 36 Visualisasi Confusion Matrix dalam bentuk heatmap 2×2 menampilkan nilai TP=16, FP=0, FN=0, TN=1 hasil pengujian.....	85

DAFTAR LAMPIRAN

Lampiran 1.1 after Kueri LogQL Lengkap untuk 13 Panel Dasbor Grafana	98
Lampiran 2. 1 Eksekusi Pemindaian Jaringan (Reconnaissance) Menggunakan Nmap	99
Lampiran 2. 2 Eksekusi Brute Force Layanan SSH (Credential Access) Menggunakan Hydra.....	99
Lampiran 2. 3 Eksekusi Akses Lateral SSH (Lateral Movement) dari Linux B ke Linux A	99
Lampiran 2. 4 Eksekusi Pemindaian Jaringan Internal (Discovery) dari Linux A ke Metasploitable 2.....	100
Lampiran 2. 5 Eksekusi Eksploitasi SQL Injection (Web Attack) Menggunakan SQLmap	100
Lampiran 2. 6 Eksekusi Eksploitasi Path Traversal Menggunakan Tool curl.....	100
Lampiran 2. 7 Eksekusi Serangan Flood Paket SYN (Denial of Service) Menggunakan hping3	100
Lampiran CV Penulis.....	101



BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi di lingkungan institusi pendidikan tinggi telah menempatkan infrastruktur jaringan sebagai tulang punggung utama dalam mendukung layanan akademik, administrasi, dan penelitian[1]. Sektor pendidikan tinggi secara konsisten menjadi salah satu target utama serangan siber, mengingat besarnya volume data sensitif yang dikelola serta ketergantungan tinggi terhadap ketersediaan layanan digital yang tidak terputus. Unit Pelaksana Teknis Pusat Teknologi Informasi dan Pangkalan Data (UPT PTIPD) UIN Sunan Kalijaga memiliki peran krusial dalam mengelola ekosistem digital tersebut melalui fasilitas Data Center yang melayani ribuan pengguna setiap harinya[2].

Hasil observasi awal pada infrastruktur jaringan PTIPD menunjukkan bahwa aktivitas trafik mencurigakan baik dari luar maupun dari dalam jaringan kampus telah teridentifikasi secara nyata, sebagaimana tercermin dari rekam jejak pemblokiran yang terdapat pada *dashboard* firewall yang beroperasi saat ini. Kondisi ini menegaskan bahwa ancaman keamanan siber terhadap Data Center Internal PTIPD bukan sekadar potensi teoretis, melainkan sebuah realitas operasional yang berlangsung secara aktif. Serangan seperti Distributed Denial of Service (DDoS), *brute force*, hingga eksploitasi celah keamanan pada lapisan aplikasi menjadi ancaman nyata yang dapat mengganggu ketersediaan layanan dan integritas data penting bagi sebuah universitas[3].

Secara topologi, jalur komunikasi data antara Edge Firewall dan Core Campus Switch pada Data Center PTIPD merupakan segmen jaringan paling strategis sekaligus rentan. Jalur ini menjadi pintu masuk utama bagi seluruh trafik dari luar menuju jaringan internal kampus maupun sebaliknya. Meskipun saat ini telah dilengkapi dengan firewall sebagai pertahanan pertama, pengamanan tersebut masih terbatas pada lapisan Network dan Transport (Layer 3 & 4). Terdapat batasan teknis di mana pengaktifan fitur Deep Packet Inspection (DPI) hingga lapisan aplikasi (Layer 7) pada perangkat firewall komersial sering kali terkendala oleh biaya lisensi yang tinggi serta risiko bottleneck yang dapat menyebabkan degradasi performa atau dropped traffic[4]. Kondisi ini menciptakan celah keamanan (*blindspot*) pada lapisan aplikasi, serta membatasi visibilitas terhadap aktivitas pergerakan serangan antar segmen (*Lateral Movement*) di dalam jaringan inti[5].

Untuk mengatasi hambatan tersebut, diperlukan sebuah sistem pertahanan tambahan yang mampu melakukan inspeksi paket secara mendalam tanpa membebani performa dan stabilitas firewall utama[6]. Suricata hadir sebagai teknologi Network Intrusion Detection System (NIDS) modern yang menawarkan kemampuan DPI pada Layer 7 secara terbuka (open-source)[7]. Dengan menempatkan Suricata secara strategis menggunakan mode AF-Packet langsung pada Core Campus Switch, administrator dapat memperoleh visibilitas lebih terhadap trafik jaringan baik dari arah eksternal maupun pergerakan lateral antar segmen VLAN internal tanpa menjadikan Suricata sebagai titik kegagalan tunggal (*single point of failure*) yang dapat mengganggu stabilitas layanan jaringan kampus. Namun, implementasi Suricata pada jaringan skala besar menghadapi tantangan dalam hal manajemen data[8]. Informasi peringatan (alerts) yang dihasilkan umumnya berupa sekumpulan log mentah (raw logs) yang masif, sehingga sulit untuk dianalisis secara cepat dan manual oleh administrator jaringan[9].

Kesenjangan visibilitas tersebut dapat dijembatani melalui integrasi sistem observabilitas menggunakan Grafana sebagai visualisasi. Grafana dipilih karena kemampuannya mengintegrasikan berbagai sumber data secara ringan dan efisien, dengan konsumsi sumber daya komputasi yang lebih rendah dibandingkan solusi alternatif seperti ELK Stack, sehingga lebih sesuai untuk lingkungan produksi yang mengutamakan stabilitas layanan. Dengan memanfaatkan stack *Monitoring* modern berupa Loki sebagai mesin penyimpanan log dan Promtail sebagai agen pengumpul log, data dari Suricata dapat diolah menjadi informasi visual yang interaktif secara *real-time*. Visualisasi ini memungkinkan identifikasi pola serangan secara intuitif, memudahkan pemantauan tren keamanan, dan mempercepat proses deteksi dini terhadap anomali trafik yang melintasi Core Switch. Penggunaan mode AF-Packet memastikan bahwa seluruh proses inspeksi tidak menjadikan sistem deteksi sebagai hambatan pada arus trafik utama[10]. Oleh karena itu, layanan di Data Center PTIPD tetap berjalan optimal meskipun sistem deteksi mengalami gangguan.

Selain aspek rancang bangun, pengukuran efektivitas terhadap sistem yang dibangun merupakan hal mutlak untuk menjamin validitas ilmiah[11]. Confusion Matrix dipilih sebagai instrumen evaluasi karena mampu memberikan gambaran komprehensif terhadap kualitas sistem deteksi, khususnya dalam mengukur keseimbangan antara ketepatan deteksi (Precision) dan kelengkapan deteksi (Recall) yang bersifat kritis dalam konteks keamanan jaringan[12]. Analisis efektivitas menggunakan parameter Precision, Accuracy, dan Recall menjadi parameter kunci dalam mengevaluasi sejauh mana ruleset Emerging Threats (ET)

Open pada Suricata mampu mendeteksi ancaman secara akurat. Melalui penelitian ini, diharapkan dapat dihasilkan sebuah sistem *Monitoring* keamanan yang komprehensif, mampu menutup celah keamanan pada lapisan aplikasi, sekaligus menyediakan representasi data yang kuat bagi pengelola infrastruktur IT di UIN Sunan Kalijaga.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disusun, maka permasalahan dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana merancang dan mengimplementasikan sistem Intrusion Detection System (IDS) berbasis Suricata dengan kombinasi ruleset Emerging Threats (ET) Open dan Custom Rules yang terintegrasi dengan ekosistem observabilitas PLG Stack (Promtail, Loki, Grafana) pada Data Center Internal PTIPD UIN Sunan Kalijaga?
2. Bagaimana efektivitas sistem deteksi intrusi berbasis Suricata dalam mendeteksi taktik serangan *East-West Traffic* berbasis *Framework* MITRE ATT&CK yang dievaluasi melalui parameter Precision, Recall, dan Accuracy menggunakan *Confusion Matrix* pada Data Center Internal PTIPD UIN Sunan Kalijaga?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Metode Pengembangan: Penelitian menggunakan kerangka kerja NDLC (Network Development Life Cycle) yang mencakup tahapan Analysis, Design, Simulation, Implementation, *Monitoring*, dan Management.
2. Metodologi Pengujian Keamanan: Prosedur pengujian keamanan menggunakan modifikasi standar Penetration Testing Execution Standard (PTES) yang dibatasi pada fase Pre-engagement, Threat Modeling, Exploitation, dan Reporting.
3. Fungsi Sistem (IDS *Non-blocking*): Sistem diimplementasikan sebagai Intrusion Detection System (IDS) tanpa fitur pemblokiran otomatis (IPS) guna menjaga ketersediaan layanan pada jaringan produksi.
4. Lingkungan dan Sumber Data: Sistem dirancang menggunakan arsitektur terdistribusi berbasis dua Virtual Machine (VM-Engine dan VM-Observability). Dengan pendekatan *Staged Deployment*, arsitektur dua VM ini diimplementasikan

terlebih dahulu di lingkungan Lab PJK untuk tahap simulasi, kemudian direplikasi secara identik di infrastruktur Data Center PTIPD untuk tahap implementasi dengan sumber data log *real-time*.

5. Cakupan Deteksi (*East-West*): Fokus utama penelitian ini adalah mengidentifikasi ancaman pergerakan serangan antar-segmen (*Inter-VLAN Lateral Movement*). Pembuktian efektivitas deteksi serangan (*Confusion Matrix*) dilakukan sepenuhnya melalui simulasi lalu lintas *East-West Traffic* di lingkungan terisolasi (*Docker Isolation*), bukan melalui eksploitasi langsung terhadap *Core Campus Switch* PTIPD. Sementara itu, untuk visibilitas ancaman pada operasional nyata, sistem diintegrasikan ke *Core Campus Switch* PTIPD hanya untuk pemantauan pasif berbasis *syslog*. Penelitian ini tidak mencakup pemantauan pada segmen DMZ.
6. Skenario Serangan: Simulasi serangan didasarkan pada *Framework* MITRE ATT&CK, mencakup taktik Reconnaissance (TA0043), Credential Access (TA0006), *Lateral Movement* (TA0008), Discovery (TA0007), Initial Access (TA0001), dan Impact (TA0040).
7. Spesifikasi Teknologi: Menggunakan Suricata v8 dengan ET Open Ruleset, Custom Rules untuk deteksi *Inter-VLAN Lateral Movement* dan stack PLG (Promtail, Loki, Grafana).
8. Parameter Evaluasi: Efektivitas diukur secara kuantitatif melalui *Confusion Matrix* (Precision, Accuracy, dan Recall) dengan unit analisis per sesi serangan. Penelitian ini tidak melakukan pengukuran langsung terhadap performa jaringan (latency/throughput) maupun penggunaan sumber daya perangkat keras (CPU/RAM).

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang dan mengimplementasikan sistem Intrusion Detection System (IDS) berbasis Suricata yang terintegrasi dengan ekosistem observabilitas PLG (Promtail, Loki, Grafana) secara *resource-efficient* menggunakan arsitektur *Staged Deployment* berbasis Virtual Machine untuk memantau lalu lintas jaringan Data Center Internal PTIPD UIN Sunan Kalijaga.

2. Menganalisis kemampuan ruleset ET Open Suricata dalam mendeteksi serangan berbasis taktik MITRE ATT&CK pada lingkungan East-West Traffic Data Center Internal PTIPD melalui skenario pengujian terkontrol berbasis standar PTES.
3. Mengevaluasi tingkat efektivitas sistem deteksi secara kuantitatif melalui instrumen Confusion Matrix guna mendapatkan nilai ukur Precision, Accuracy, dan Recall sebagai dasar rekomendasi kelayakan sistem.

1.5 Manfaat Penelitian

1.5.1 Bagi Institusi (UPT PTIPD UIN Sunan Kalijaga)

- Menutup Celah Keamanan (*Blindspot*): Memberikan purwarupa (prototype) sistem deteksi yang mampu melakukan Deep Packet Inspection (DPI) pada Layer 7, sehingga memberikan visibilitas penuh terhadap pergerakan lateral (*Lateral Movement*) yang selama ini tidak terjangkau oleh firewall tradisional.
- Solusi Efisien dan Ekonomis: Menawarkan sistem pertahanan tambahan berbasis teknologi open-source yang bekerja secara terpisah tanpa membebani kinerja perangkat firewall utama. Solusi ini memberikan perlindungan sekilas enterprise tanpa mewajibkan institusi mengeluarkan biaya lisensi DPI yang tinggi.
- Manajemen Insiden yang Terstruktur: Menyediakan visualisasi (Grafana) yang interaktif, mengubah log mentah (raw logs) menjadi informasi siap tindak (actionable intelligence) guna mempercepat proses identifikasi dan mitigasi ancaman oleh administrator jaringan.

1.5.2 Bagi Ilmu Pengetahuan dan Akademik

- Referensi Arsitektur Keamanan: Menjadi literatur akademis mengenai penerapan paradigma *Assume breach* dan pentingnya pengamanan East-West Traffic pada arsitektur jaringan kampus skala besar.
- Validasi Emulasi Serangan: Memberikan panduan empiris mengenai penerapan simulasi serangan berbasis standar *Framework* MITRE ATT&CK di lingkungan terkontrol yang dapat direplikasi untuk penelitian keamanan siber selanjutnya.

1.5.3 Bagi Peneliti

- Peningkatan Kompetensi Profesional: Memperdalam keahlian praktis dalam bidang Network Security Engineering, khususnya pada tahapan Network Development Life Cycle (NDLC), manajemen log skala besar, dan konfigurasi infrastruktur keamanan berbasis kontainerisasi.



BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan pada Data Center Internal PTIPD UIN Sunan Kalijaga, penelitian ini menjawab dua rumusan masalah sebagai berikut.

1. Rancang bangun sistem Intrusion Detection System (IDS) berbasis Suricata yang terintegrasi dengan ekosistem observabilitas PLG Stack (Promtail, Loki, Grafana) telah berhasil diimplementasikan secara *resource-efficient* menggunakan arsitektur *Staged Deployment* berbasis dua Virtual Machine (VM-Engine dan VM-Observability). Sistem beroperasi secara pasif (*non-blocking*) melalui mode AF-Packet, dengan simulasi skenario Inter-VLAN *Lateral Movement* dilaksanakan pada lingkungan terisolasi Docker Bridge Network, sementara pemantauan trafik nyata Data Center dilakukan melalui interface ENS yang membaca syslog Core Campus Switch. Pengembangan Custom Rules (SID 9001001–9007003) terbukti menutupi celah deteksi (*blindspot*) ET Open Ruleset khususnya pada validasi pola SSH pivot lintas-subnet sebagai representasi Inter-VLAN *Lateral Movement* (MITRE T1021.004) melalui satu skenario terkontrol (Skenario 3). Generalisasi terhadap teknik pergerakan lateral lain memerlukan pengujian lanjutan sebagaimana disarankan pada sub-bab 5.2.

2. Efektivitas sistem deteksi terhadap taktik serangan East-West Traffic berbasis *Framework* MITRE ATT&CK, yang diukur melalui instrumen Confusion Matrix, menunjukkan nilai Precision, Recall, dan Accuracy masing-masing sebesar 100% dari 16 sesi serangan yang teridentifikasi sebagai True Positive tanpa satu pun False Positive maupun False Negative. Custom Rules memberikan kontribusi dominan sebesar 62,5% (10 dari 16 sesi) dibandingkan ET Open Ruleset sebesar 37,5%, termasuk kontribusi eksklusif pada deteksi pola SSH pivot antar-subnet yang tidak tercakup oleh ruleset publik. Perlu ditegaskan bahwa nilai evaluasi sempurna ini merepresentasikan keberhasilan sistem pada skenario dan kondisi pengujian terkontrol yang dirancang (*proof of concept*), bukan jaminan generalisasi performa pada seluruh kondisi operasional Data Center PTIPD, mengingat

keterbatasan jumlah sampel pengujian dan cakupan kebijakan forwarding syslog yang telah diuraikan pada sub-bab 4.6.5.

5.2 Saran

Berdasarkan keterbatasan yang telah diidentifikasi pada sub-bab 4.6.5, penelitian selanjutnya disarankan untuk mempertimbangkan beberapa hal berikut guna memperkuat validitas dan generalisasi temuan.

1. Perluasan Durasi Observasi Kondisi Tenang: Pengumpulan *baseline* data lalu lintas normal (Kondisi Tenang) pada penelitian ini dibatasi hanya satu hari akibat keterbatasan kapasitas penyimpanan Virtual Machine. Penelitian selanjutnya disarankan memperpanjang durasi observasi trafik normal kampus untuk memperkuat validitas statistik nilai Precision dan Accuracy terhadap kemungkinan False Positive dalam jangka waktu operasional yang lebih panjang.

2. Penambahan Cakupan Skenario Serangan: Penelitian ini terbatas pada tujuh skenario serangan berbasis lima taktik MITRE ATT&CK. Penelitian lanjutan perlu memperluas vektor pengujian, khususnya untuk taktik *Lateral Movement*, dengan mencakup protokol lain seperti SMB, RDP, atau WMI yang umum dimanfaatkan dalam serangan Advanced Persistent Threat (APT), guna menguji generalisasi Custom Rules di luar pola SSH pivot yang telah divalidasi.

3. Pengukuran Dampak Performa Jaringan: Penelitian ini tidak mengukur dampak operasional Suricata mode AF-Packet terhadap performa jaringan. Penelitian lanjutan disarankan melakukan stress-testing terukur untuk mengevaluasi indikator penurunan throughput atau peningkatan latency pada kondisi beban puncak (peak hours), khususnya sebagai syarat kelayakan sebelum Rekomendasi 1 (*deployment* produksi pada Core Campus Switch, sub-bab 4.6.4) dapat diterapkan secara penuh.

DAFTAR PUSTAKA

- [1] Y. A. Nugroho, A. Widodo, E. T. Pebrina, J. Iskandar, and M. Nadeak, "Digitalization in Higher Education: How Information Systems Improve Operational and Strategic Performance," *Indonesian Journal of Management and Economic Research*, 2025.
- [2] P. Sahrial, D. Arsa, P. Eko Prasetyo Utomo, D. Suprayogi, M. Ilhami, and U. Jambi, "PEMELIHARAAN DAN PELATIHAN TROUBLESHOOT JARINGAN KOMPUTER UNTUK PENINGKATAN LAYANAN AKADEMIK UNIVERSITAS JAMBI," 2025.
- [3] A. R. Syujak, K. Diantoro, V. Yuni T, A. Soderi, and P. A. Sucipto, "Integrasi Deep Packet Inspection dengan Intrusion Detection System (IDS) untuk Identifikasi Serangan DDoS dalam Jaringan Skala Besar," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1971–1975, Dec. 2024, doi: 10.33395/jmp.v13i2.14324.
- [4] H. Haugerud, H. N. Tran, N. Aitsaadi, and A. Yazidi, "A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization," *Future Generation Computer Systems*, vol. 124, pp. 254–267, Nov. 2021, doi: 10.1016/j.future.2021.05.037.
- [5] 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, Jan. 2026, doi: 10.33395/sinkron.v10i1.15616.
- [6] D. A. Saputra, S. Deris, and S. Tata, "Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang," *Indonesian Journal of Multidisciplinary on Social and Technology*, vol. 1, no. 2, pp. 176–183, Jun. 2023, doi: 10.31004/ijmst.v1i2.142.
- [7] H. Asad, S. Adhikari, and I. Gashi, "A perspective–retrospective analysis of diversity in *signature-based* open-source network intrusion detection systems," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1331–1346, Apr. 2024, doi: 10.1007/s10207-023-00794-9.
- [8] D. H. K. Raharjo and Muhammad Salman, "ANALYZING SURICATA ALERT DETECTION PERFORMANCE ISSUES BASED ON ACTIVE INDICATOR OF COMPROMISE RULES," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 3, pp. 601–610, Jun. 2023, doi: 10.52436/1.jutif.2023.4.3.1013.

- [9] N. Murali Krishna Koneru, "Centralized Logging and Observability in AWS-Implementing ELK Stack for Enterprise Applications," *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 2, May 2025, doi: 10.22399/ijcesen.2289.
- [10] OISF (Open Information Security Foundation), "Suricata User Guide," 2026.
- [11] R. Ahmad and M. Saiful, "Analisis Komparatif Feture Selection dan Metode Klasifikasi Intrution Detection System (IDS)," *Infotek: Jurnal Informatika dan Teknologi*, vol. 8, no. 2, pp. 673–685, Jul. 2025, doi: 10.29408/jit.v8i2.31103.
- [12] A. Suryadi and M. I. Marzuki, "Pengembangan Intrusion Detection System (Ids) Berbasis Machine Learning," *InComTech : Jurnal Telekomunikasi dan Komputer*, vol. 13, no. 3, pp. 189–195, Dec. 2023, doi: 10.22441/incomtech.v13i3.15118.
- [13] M. Sheeraz, M. H. Durad, M. A. Paracha, S. M. Mohsin, S. N. Kazmi, and C. Maple, "Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection," *Sensors*, vol. 24, no. 15, Aug. 2024, doi: 10.3390/s24154901.
- [14] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
- [15] Z. Long, H. Yan, G. Shen, X. Zhang, H. He, and L. Cheng, "A Transformer-based network intrusion detection approach for cloud security," *Journal of Cloud Computing*, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-023-00574-9.
- [16] A. Gurajapu and V. Garimella, "Secure Service-Mesh implementations: Mitigating lateral-movement risks in container-based Telecom Apps," *International Journal of Research Publications in Engineering, Technology and Management*, vol. 8, no. 1, Feb. 2025, doi: 10.15662/IJRPETM.2025.0801010.
- [17] N. I. C. Mat, N. Jamil, Y. Yusoff, and M. L. M. Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," 2024, *Oxford University Press*. doi: 10.1093/cybsec/tyad023.
- [18] A. Mohile, "Next-Generation Firewalls: A Performance-Driven Approach to Contextual Threat Prevention," *International Journal of Computer Technology and Electronics Communication*, vol. 06, no. 01, Feb. 2023, doi: 10.15680/IJCTECE.2023.0601003.
- [19] H. J. Hadi *et al.*, "iKern: Advanced Intrusion Detection and Prevention at the Kernel Level Using eBPF," *Technologies (Basel)*, vol. 12, no. 8, Aug. 2024, doi: 10.3390/technologies12080122.

- [20] J. E. Varghese and B. Muniyal, "An Efficient IDS *Framework* for DDoS Attacks in SDN Environment," *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.
- [21] A. H. Janabi, T. Kanakis, and M. Johnson, "Survey: Intrusion Detection System in Software-Defined Networking," *IEEE Access*, vol. 12, pp. 164097–164120, 2024, doi: 10.1109/ACCESS.2024.3493384.
- [22] T. Zhukabayeva, Z. Ahmad, A. Adamova, N. Karabayev, and A. Abdildayeva, "An Edge-Computing-Based Integrated *Framework* for Network Traffic Analysis and Intrusion Detection to Enhance Cyber–Physical System Security in Industrial IoT," *Sensors*, vol. 25, no. 8, Apr. 2025, doi: 10.3390/s25082395.
- [23] F. Luqman, H. Danang Rimbawa, and N. Wibisono, "Implementasi Extended Detection and Response pada Security Operation Center dan Computer Security Independent Response Team dalam Peningkatan Sistem Keamanan Informasi Guna Meningkatkan Sistem Pertahanan Informasi," *VISA: Journal of Visions and Ideas*, vol. 5, no. 3, p. 1215, 2025.
- [24] M. Hassan, M. E. Haque, M. E. Tozal, V. Raghavan, and R. Agrawal, "Intrusion Detection Using Payload Embeddings," *IEEE Access*, vol. 10, pp. 4015–4030, 2022, doi: 10.1109/ACCESS.2021.3139835.
- [25] Dhuha Sabri Ghazi, H. S. Hamid, M. J. Zaiter, and A. S. Ghazi Behadili, "Snort Versus Suricata in Intrusion Detection," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 2, pp. 73–88, Dec. 2024, doi: 10.31987/ijict.7.2.290.
- [26] G. Kudjo Bada, W. K. Nabare, D. Kwame, and K. Quansah, "Comparative Analysis of the Performance of Network Intrusion Detection Systems: Snort, Suricata and Bro Intrusion Detection Systems in Perspective," 2020.
- [27] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144759.
- [28] P. Singh, A. Kaur, G. Singh Aujla, S. Batth, and S. Kanhere, "IEEE INTERNET OF THINGS JOURNAL 1 DaaS: Dew Computing as a Service for Intelligent Intrusion Detection in Edge-of-Things Ecosystem," 2020.
- [29] Y. Chen, S. Layeghy, L. D. Manocchio, and M. Portmann, "P4-NIDS: High-Performance Network *Monitoring* and Intrusion Detection in P4," Dec. 2024, [Online]. Available: <http://arxiv.org/abs/2411.17987>

- [30] Z. Zulkhakim and A. Kurniawan, "Implementasi Continuous Integration Dan Continuous *Deployment* Pada Pengembangan Aplikasi Website Menggunakan Docker Dan Github Actions," *Jurnal Manajemen Informatika*, vol. 16, no. 01, 2024.
- [31] D. Dervinis, "Energy and resource modeling: A comparative analysis of containers and virtual machines," *PROFESSIONAL STUDIES: Theory And Practice*, vol. 28, no. 2, pp. 29–34, 2024.
- [32] K. S. Arlandy, A. Faqih, and A. R. Rinaldi, "Mengoptimalkan Kinerja Naïve Bayes Pada Ancaman Modern Dengan Menggunakan PCA Pada Data Intrusion Detection System (IDS)," 2025.
- [33] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *Journal of Cloud Computing*, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-024-00685-x.
- [34] M. K. Suryadewiansyah, T. Endra, and E. Tju, "Jurnal Nasional Teknologi dan Sistem Informasi Naïve Bayes dan Confusion Matrix untuk Efisiensi Analisa Intrusion Detection System Alert," 2022, doi: 10.25077/TEKNOSI.v8i2.2022.081-088.
- [35] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced Intrusion Detection Systems Performance with UNSW-NB15 Data Analysis," *Algorithms*, vol. 17, no. 2, Feb. 2024, doi: 10.3390/a17020064.