



**OPTIMALISASI ANALISIS ANCAMAN SIBER SOC
MENGUNAKAN SISTEM SIEM QRADAR TERINTEGRASI
LLM GEMINI BERBASIS WEB**

**TUGAS AKHIR
SKRIPSI**

SAMPUL

ARVIAN SYIDDIQ

41522010243

**UNIVERSITAS
MERCU BUANA**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2026



**OPTIMALISASI ANALISIS ANCAMAN SIBER SOC
MENGUNAKAN SISTEM SIEM QRADAR TERINTEGRASI
LLM GEMINI BERBASIS WEB**

**TUGAS AKHIR
SKRIPSI**

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana

Arvian Syiddiq

41522010243

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2026

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Arvian Syiddiq

NIM : 41522010243

Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika

Menyatakan dengan sebenar-benarnya bahwa Tugas Akhir berjudul:

“Optimalisasi Analisis Ancaman Siber SOC Menggunakan Sistem SIEM Qradar terintegrasi LLM Gemini Berbasis Web” adalah hasil karya saya sendiri, tidak mengandung unsur plagiarisme, pelanggaran hak cipta, atau konten ilegal dalam bentuk apapun dan tidak melanggar hukum atau hak pihak manapun.

Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menanggung seluruh konsekuensi hukum dan membebaskan Universitas Mercu Buana dari segala bentuk tuntutan hukum dan saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Jakarta, 30 Juli 2026



Arvian Syiddiq

PERNYATAAN SIMILARITY CHECK
/SIMILARITY CHECK STATEMENT

Saya yang bertanda tangan dibawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh
/The undersigned, hereby declare that the scientific work written by

Nama /Name : Arvian Syiddiq
NIM /Student ID Number : 41522010243
Program Studi /Study Program : Teknik Informatika

Dengan Judul Tugas Akhir

/The title:

“Optimalisasi Analisis Ancaman Siber SOC Menggunakan Sistem SIEM Qradar terintegrasi LLM Gemini Berbasis Web ”

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal:

/Similarity checks have been carried out with the Turnitin system on the date:

21 Juli 2026

dengan nilai persentase sebesar :

/with a percentage value of:

16%

dinyatakan memenuhi standar sesuai dengan ketentuan berlaku di **Fakultas Ilmu Komputer** Universitas Mercu Buana. */declared to meet standards in accordance with applicable regulations at the Faculty of Computer Science, Universitas Mercu Buana.*

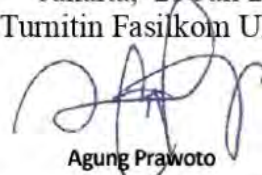
File hasil cek similarity turnitin:

/Turnitin similarity report file

https://drive.google.com/file/d/18WJg9tcyV5E_nv0FR5cfiktJx7ZMOk66/view?usp=drive_link



Jakarta, 21 Juli 2026
Admin Turnitin Fasilkom UMB



Agung Prawoto

Agung Prawoto, S.Kom., B.Sc

NIK : 322970503

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : ARVIAN SYIDDIQ
NIM : 41522010243
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika
Judul Tugas Akhir : Optimalisasi Analisis Ancaman Siber SOC
Menggunakan Sistem SIEM Qradar terintegrasi LLM
Gemini Berbasis Web

Telah berhasil dipertahankan pada sidang tanggal 30 Juli 2026 dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing



Muhammad Ali Akbar, S.SI., M.Kom

NIDN/NUPTK: 0415058501

Jakarta, 30 Juli 2026

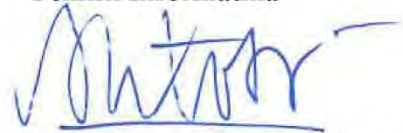
Mengetahui,

Dekan Fakultas Ilmu Komputer



Dr. Bambang Jokonowo, S.Si., MTI
NIDN/NUPTK: 0320037002

Ketua Program Studi
Teknik Informatika



Dr. Hadi Santoso, S.Kom., M.Kom
NIDN/NUPTK: 0225067701

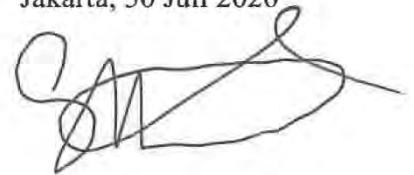
KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Tugas Akhir ini. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Informatika pada Fakultas Ilmu Komputer Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Tugas Akhir ini, sangatlah sulit bagi saya untuk menyelesaikan Tugas Akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana.
4. Bapak/Ibu Dosen Pembimbing selaku dosen pembimbing tugas akhir yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan tugas akhir ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercu Buana.
6. Teman-teman saya yang telah memberikan dukungan, semangat, motivasi, serta bantuan selama proses perkuliahan hingga penyusunan tugas akhir ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Tugas Akhir ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 30 Juli 2026



Arvian Syiddiq

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : ARVIAN SYIDDIQ
NIM : 41522010243
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika
Judul Laporan Skripsi : Optimalisasi Analisis Ancaman Siber SOC
Menggunakan Sistem SIEM Qradar
terintegrasi LLM Gemini Berbasis Web

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 30 Juli 2026

Yang menyatakan,



Arvian Syiddiq

OPTIMALISASI ANALISIS ANCAMAN SIBER SOC MENGUNAKAN SISTEM SIEM QRADAR TERINTEGRASI LLM GEMINI BERBASIS WEB

ARVIAN SYIDDIQ

ABSTRAK

Security Operations Center (SOC) memiliki peran penting dalam mendeteksi dan merespons ancaman siber melalui pemanfaatan sistem *Security Information and Event Management (SIEM)*. Namun, tingginya *volume alert* dan kompleksitas log keamanan sering menimbulkan *alert fatigue* yang berdampak pada meningkatnya waktu triase serta beban kerja analis SOC. Penelitian ini bertujuan untuk mengoptimalkan proses analisis ancaman siber dengan mengintegrasikan IBM QRadar SIEM dan *Large Language Model (LLM)* Gemini ke dalam sebuah sistem berbasis web yang mampu melakukan analisis *offense* secara otomatis. Metode penelitian yang digunakan meliputi perancangan dan pengembangan sistem terintegrasi menggunakan QRadar API dan Gemini API, serta pengujian secara kuantitatif melalui pendekatan eksperimen komparatif. Sistem yang dikembangkan mampu mengambil data *offense* secara otomatis, menghasilkan ringkasan insiden, mengklasifikasikan tingkat ancaman, serta menyajikan hasil analisis melalui dashboard web interaktif untuk mendukung proses triase pada lingkungan SOC. Pengujian dilakukan menggunakan dataset *offense* yang diperoleh dari lingkungan perusahaan dengan *retention* log selama satu bulan. Hasil evaluasi menunjukkan bahwa sistem mampu mengklasifikasikan ancaman dengan nilai *Accuracy* sebesar 88,04%, *Recall* sebesar 88,37%, *Precision* sebesar 73,01%, *F1-Score* sebesar 0,80, dan *Specificity* sebesar 87,92%. Selain itu, sistem berhasil mengotomatisasi proses analisis log serta menyajikan ringkasan insiden yang relevan dan mudah dipahami, sehingga membantu analis memahami konteks ancaman dengan lebih cepat dan efisien. Berdasarkan hasil penelitian, integrasi IBM QRadar SIEM dan Gemini LLM terbukti efektif dalam mendukung analisis ancaman siber pada *Security Operations Center*. Sistem yang dikembangkan mampu meningkatkan efektivitas klasifikasi ancaman, mempercepat proses triase insiden, serta mengurangi beban kerja analis SOC melalui penyajian analisis keamanan yang terstruktur dan otomatis.

Kata kunci: *Security Operations Center*, SIEM, IBM QRadar, *Large Language Model*, Gemini AI, Analisis Ancaman Siber, *Threat Detection*.

OPTIMALISASI ANALISIS ANCAMAN SIBER SOC MENGUNAKAN SISTEM SIEM QRADAR TERINTEGRASI LLM GEMINI BERBASIS WEB

ARVIAN SYIDDIQ

ABSTRACT

Security Operations Centers (SOCs) play a critical role in detecting and responding to cyber threats through the utilization of Security Information and Event Management (SIEM) systems. However, the high volume of security alerts and the complexity of log data often lead to alert fatigue, resulting in increased triage time and analyst workload. This study aims to optimize cyber threat analysis by integrating IBM QRadar SIEM with the Gemini Large Language Model (LLM) into a web-based system capable of performing automated offense analysis. The research methodology includes the design and development of an integrated system utilizing QRadar API and Gemini API, followed by quantitative evaluation through a comparative experimental approach. The developed system is capable of automatically retrieving offense data, generating incident summaries, classifying threat levels, and presenting analysis results through an interactive web dashboard to support incident triage activities within a SOC environment. The evaluation was conducted using offense datasets collected from an operational enterprise environment with a one-month log retention period. The results demonstrate that the system achieved an Accuracy of 88.04%, Recall of 88.37%, Precision of 73.01%, F1-Score of 0.80, and Specificity of 87.92%. Furthermore, the system successfully automated the log analysis process and produced relevant, easy-to-understand incident summaries, enabling security analysts to understand threat contexts more efficiently. Based on the findings, the integration of IBM QRadar SIEM and the Gemini Large Language Model proved effective in supporting cyber threat analysis within a Security Operations Center. The developed system improved threat classification performance, accelerated incident triage processes, and reduced analyst workload through structured and automated security analysis.

Keywords: *Security Operations Center, SIEM, IBM QRadar, Large Language Model, Gemini AI, Cyber Threat Analysis, Threat Detection.*

DAFTAR ISI

HALAMAN SAMPUL.....	0
HALAMAN JUDUL	i
HALAMAN PERNYATAAN KARYA SENDIRI	ii
HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN	iii
HALAMAN PENGESAHAN.....	iv
KATA PENGANTAR.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB.....	vi
ARVIAN SYIDDIQ.....	vii
ABSTRAK	vii
ARVIAN SYIDDIQ.....	viii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian.....	3
1.4 Batasan Penelitian.....	3
1.5 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Teori Utama	6
2.1.1 Large Language Model (LLM)	6
2.1.2 Prompt Engineering	6
2.1.3 Security Operations Center (SOC).....	7
2.1.4 SIEM & IBM QRadar	8
2.2 Teori Pendukung	8
2.1.5 Python & Backend	8
2.1.6 React & Frontend	9
2.1.7 API	9
2.3 Penelitian Terdahulu	10
2.4 Gap Penelitian	35
BAB III METODE PENELITIAN	36
3.1 Pendekatan Penelitian	36
3.2 Desain Penelitian.....	36
3.3 Subject Penelitian.....	38
3.4 Instrumen Penelitian.....	38
3.4.1 IBM QRadar SIEM & QRadar API	38
3.4.2 LLM Gemini API	39

3.4.3	Sistem SIEM–LLM.....	39
3.4.4	Stopwatch / Time-Tracking Tool.....	39
3.4.5	Lembar Pencatatan Hasil Triase.....	39
3.4.6	Lembar Ground Truth	39
3.5	Teknik Pengumpulan Data.....	40
3.5.1	Ground Truth Preparation	40
3.5.2	Perbandingan dengan Ground Truth	40
3.6	Analisis Data	41
3.6.1	Analisis Pengujian Fungsional Sistem.....	41
3.6.2	Analisis Respon Analisis AI.....	42
3.6.3	Analisis Performa Sistem.....	43
3.7	Prosedur Penelitian.....	45
3.7.1	Identifikasi Masalah dan Studi Literatur.....	45
3.7.2	Perancangan Sistem Aplikasi	46
3.7.3	Integrasi dan Pengembangan Web	51
3.7.4	Pengujian Sistem dan Pengumpulan Data	51
3.7.5	Analisis dan Visualisasi Data	51
3.7.6	Penyusunan Laporan dan Kesimpulan.....	52
3.8	Evaluasi Hasil Penelitian.....	52
3.9	Timeline Penelitian	53
3.9.1	Persiapan Penelitian	53
3.9.2	Studi Literatur	53
3.9.3	Perancangan Sistem	53
3.9.4	Pengembangan Sistem	53
3.9.5	Pengujian Sistem.....	54
3.9.6	Penulisan Laporan.....	54
BAB IV PEMBAHASAN.....		55
4.1	Gambaran Umum.....	55
4.1.1	Mengambil data offense dari IBM QRadar secara otomatis.....	55
4.1.2	Analisis offense berbasis AI menggunakan Gemini LLM.....	56
4.1.3	Menghasilkan ringkasan insiden secara otomatis	57
4.1.4	Mengklasifikasikan tingkat ancaman.....	57
4.1.5	Menampilkan hasil analisis melalui Dashboard web interaktif	57
4.1.6	Mendukung efisiensi proses triase SOC	57
4.2	Implementasi	58
4.2.1	Interface Pengguna.....	58
4.2.2	Proses Bisnis Sistem	60

4.2.3	Arsitektur Backend.....	61
4.3	Evaluasi Sistem	63
4.3.1	Pengujian fungsional sistem.....	63
4.3.2	Analisis Respon Analisis AI.....	64
4.3.3	Evaluasi Metrik	65
4.4	Diskusi Hasil Penelitian	73
4.4.1	Kelebihan Sistem	73
4.4.2	Keterbatasan Sistem	75
4.4.3	Rekomendasi Pengembangan.....	76
BAB V KESIMPULAN DAN SARAN		78
5.1	Kesimpulan	78
5.2	Saran.....	79
DAFTAR PUSTAKA		80
LAMPIRAN.....		84



DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	10
Tabel 3.1 Rancangan Database	50
Tabel 4.1 Hasil Pengujian Fungsionalitas Sistem	64
Tabel 4.2 Data Ground Truth	66
Tabel 4.3 Hasil Evaluasi	68



DAFTAR GAMBAR

Gambar 3.1 Desain Penelitian.....	37
Gambar 3.2 Usecase Diagram.....	46
Gambar 3.3 Sequence Diagram.....	48
Gambar 4.1 Promp	56
Gambar 4.2 High Level Structure	58
Gambar 4.3 Dashboard.....	59
Gambar 4.4 Hasil Analisis Offense.....	59
Gambar 4.5 Hasil Analisis Offense.....	59
Gambar 4.6 Hasil Email Notifier	60
Gambar 4.7 Hasil Respon Analisis	65
Gambar 4.8 Diagram Confusion Matrix	67
Gambar 4.9 Visualisasi Hasil Evaluasi Performance Metrix.....	72
Gambar 4.10 Visualisasi Mean Time To Triage.....	72



DAFTAR LAMPIRAN

Lampiran 1. Kartu Asistensi	84
Lampiran 2. CV.....	85
Lampiran 3. Surat Pernyataan & Pengalihan HAKI	86
Lampiran 4. Surat Keterangan Mengikuti BNSP.....	88
Lampiran 5. Surat Izin Riset Perusahaan	89

