Buletin Ilmiah
Ilmu Komputer dan Multimedia

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

Perancangan dan Implementasi Sistem SOAR Dengan Integrasi AI Gemini Untuk Rekomendasi Mitigasi Di Universitas Terbuka

Muhammad Alfian Nurrizky[1], Sutriyono[2*]

[1,2]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]alfiannrzky0@gmail.com, [2*]dosen02346@unpam.ac.id
(* : coressponding author)

Abstrak− Universitas Terbuka adalah lembaga pendidikan yang membutuhkan sistem yang efisien untuk mengelola dan merespons ancaman siber. Sebelumnya, penanganan insiden keamanan siber dilakukan secara manual, yang sering menyebabkan ketidaksesuaian dalam pengelompokan peringatan, risiko keterlambatan dalam respons, serta rendahnya efisiensi kerja tim keamanan. Penelitian ini bertujuan untuk mengembangkan sistem Security Orchestration, Automation, and Response (SOAR) yang dapat mendukung Universitas Terbuka dalam mendeteksi, memperkaya, dan merespons insiden siber secara terstruktur dan langsung, termasuk penggunaan AI Gemini untuk memberikan rekomendasi penanggulangan. Pendekatan yang digunakan dalam pengembangan sistem ini adalah metode Prototype, yang terdiri dari beberapa tahap seperti pengumpulan kebutuhan, perancangan awal, pembuatan prototype, pengujian oleh pengguna, serta perbaikan berulang. Hasil pengembangan sistem SOAR menunjukkan peningkatan efisiensi kerja tim keamanan dalam memproses insiden, pengurangan kesalahan pada proses pengelompokan peringatan, serta peningkatan kecepatan respons. Sistem ini juga membantu manajer keamanan dalam melakukan pemantauan dan evaluasi penanganan insiden secara lebih akurat dan terbuka.

Kata Kunci: Soar, Insiden Siber, Efisiensi, AI Gemini, *Prototype*

Abstrack− *Universitas Terbuka is an educational institution requiring an efficient system to manage and respond to cyber threats. Previously, cybersecurity incidents were handled manually, often leading to inconsistencies in alert grouping, the risk of delays in response, and low security team efficiency. This research aims to develop a Security Orchestration, Automation, and Response (SOAR) system that can support Universitas Terbuka in detecting, enriching, and responding to cyber incidents in a structured and immediate manner, including the use of Gemini AI to provide countermeasure recommendations. The approach used in developing this system is the Prototype method, which consists of several stages such as requirements gathering, initial design, prototyping, user testing, and iterative improvements. The results of the SOAR system development show an increase in the security team's efficiency in processing incidents, a reduction in errors in the alert grouping process, and an increase in response speed. This system also helps security managers monitor and evaluate incident handling more accurately and transparently.*

Keywords: *Soar, Cyber Incident, Efficiency, Gemini AI, Prototype*

1. PENDAHULUAN

Dengan berkembangnya teknologi, tidak berarti tidak ada masalah. Teknologi internet juga bisa menjadi sarana untuk kejahatan yang disebut cyber crime. Semakin cepat orang menggunakan teknologi, semakin tinggi risiko terjadinya tindakan kriminal oleh pihak yang tidak bertanggung jawab, seperti penipuan, pencurian, pencemaran nama baik, dan tindakan kejahatan lainnya melalui internet. Manajemen aset diartikan sebagai proses yang terorganisir untuk merawat, memperbarui, dan mengoperasikan aset secara efektif dan efisien, sehingga mendukung tujuan strategis perusahaan. Jika pengelolaan aset tidak dilakukan dengan baik, dapat menyebabkan inefisiensi, hilangnya aset, serta penurunan produktivitas secara keseluruhan [1].

Universitas Terbuka, sebagai salah satu perguruan tinggi negeri yang terkemuka, menghadapi tantangan besar dalam mengelola dan merespons insiden keamanan siber yang dapat mengganggu integritas data dan kelangsungan operasional [2]. Saat ini, proses penanganan peringatan keamanan dan insiden masih dilakukan secara manual atau hanya mengandalkan otomasi terbatas. Hambatan seperti kurangnya integrasi antar alat keamanan, belum adanya otomatisasi dalam proses triase, serta minimnya panduan respons yang cepat, mengakibatkan lambatnya proses

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

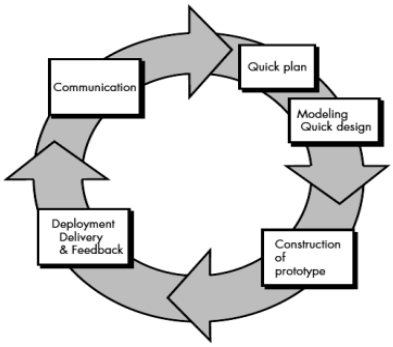
investigasi dan meningkatnya kelelahan tim keamanan akibat banyaknya peringatan yang harus ditangani (alert fatigue)

Untuk menghadapi tantangan tersebut, dibutuhkan pengembangan sistem otomatisasi yang akurat, efisien, dan terintegrasi. Penelitian sebelumnya telah menunjukkan bahwa implementasi sistem orchestration, automation, dan response (SOAR) dalam keamanan berhasil meningkatkan notifikasi keamanan secara real-time. Desain sistem ini diharapkan mampu mengubah proses manual menjadi alur kerja digital yang otomatis, meningkatkan keakuratan dalam mendeteksi dan merespons ancaman, serta memberikan akses informasi peristiwa keamanan dan rekomendasi mitigasi secara langsung kepada tim keamanan. Dengan demikian, perusahaan dapat meningkatkan efisiensi dan produktivitas secara signifikan [3].

2. METODE PENELITIAN

2.1 Metode Penelitian

Penelitian ini menggunakan pendekatan prototype sebagai metode desain sistem. Model prototype adalah sebuah metode di mana pengembang perangkat lunak membuat mockup berupa model aplikasi. Metode ini sangat cocok digunakan ketika pengguna tidak dapat menjelaskan secara jelas kebutuhan yang sesuai dengan harapan mereka [4]. Metode pengembangan sistem model prototype adalah salah satu pendekatan umum yang digunakan dalam pengembangan perangkat lunak. [4].



Gambar 1. Langkah-Langkah Metode *Prototype*

1. *Communication*: Pada tahap ini dilakukan identifikasi kebutuhan pengguna, proses ini bertujuan agar penulis dapat memperoleh informasi mengenai masalah yang dialami oleh klien. Data yang diperoleh dari masalah tersebut nantinya digunakan sebagai pedoman dalam proses pencarian solusi dan pengembangan pada tahap berikutnya.
2. *Quick Plan*: Pada tahap ini, perancangan dilakukan dengan cepat dan mencakup semua aspek perangkat lunak yang sudah diketahui, serta rancangan tersebut berfungsi sebagai dasar dalam membuat prototype.
3. *Modelling Quick Design*: Di tahap ini fokusnya adalah pada bagian perangkat lunak yang bisa dilihat oleh pelanggan atau pengguna. Modelling Quick Design lebih menekankan pada pembuatan prototype [5].
4. *Construction of Prototype* : Pembuatan perangkat *prototype* termasuk pengujian dan penyempurnaan [5].
5. *Delivery & Feedback* : Tahap penyerahan sistem ke pengguna dan umpan balik [5].

3. ANALISA DAN PEMBAHASAN

3.1 Analisis Kebutuhan Sistem

Berdasarkan Berdasarkan hasil wawancara, diperlukan sistem orchestration, automation, dan response security untuk memudahkan proses pencatatan dan pelaporan insiden keamanan siber. Sistem ini juga bertujuan meminimalkan kesalahan dalam proses triase dan respons. Selain itu,

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

sistem harus mampu digunakan untuk mencatat detail insiden, indikator kompromi, langkah-langkah mitigasi yang diambil, serta waktu kejadian dan cara penanganannya.

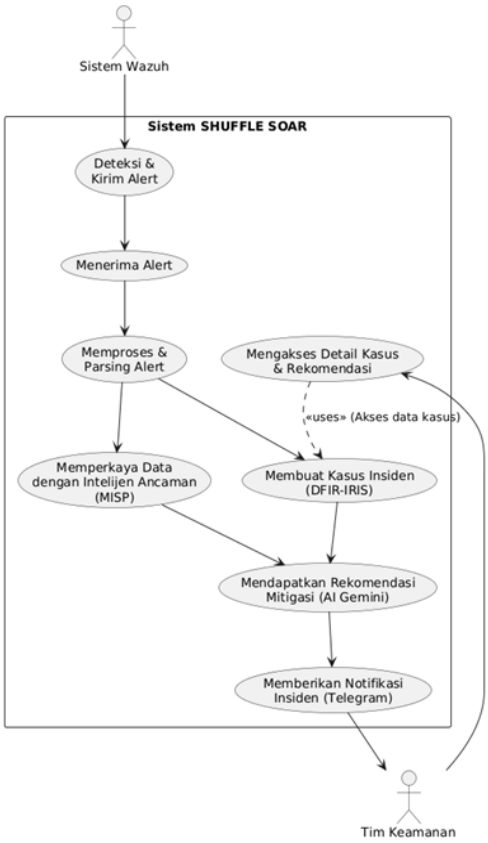
3.2 Perancangan Sistem

Sistem dirancang menggunakan Unified Modeling Language (UML), yang bertujuan untuk memudahkan proses penjelasan dan pembuatan desain sistem perangkat lunak, terutama sistem yang dikembangkan dengan pendekatan pemrograman berorientasi objek. UML dikembangkan melalui penggabungan berbagai bahasa pemodelan grafis berorientasi objek yang berkembang cepat di akhir tahun 1980-an dan awal tahun 1990-an [6].

3.2.1 *Use Case Diagram*

Use Case Diagram adalah gambar yang digunakan untuk menunjukkan semua kegiatan yang dilakukan oleh sistem dari perspektif pengguna [5]. Ini adalah diagram yang digunakan untuk mengetahui kebutuhan fungsional dari sistem manajemen alat.

a. *Use Case Workflow SOAR*



Gambar 2. *Use Case Diagram* SOAR

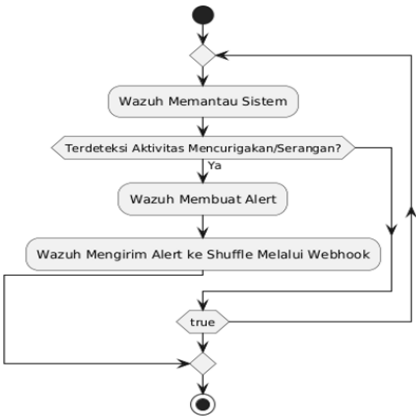
Use case diagram ini menjelaskan peran Sistem SOAR dalam sistem manajemen perangkat, yaitu menerima peringatan dari Wazuh, memproses dan memperkaya data insiden dengan menggunakan intelijen ancaman dari MISP, membuat laporan kasus insiden di DFIR-IRIS, memberikan rekomendasi mitigasi berdasarkan AI Gemini, serta mengirimkan pemberitahuan ke tim keamanan.

3.2.2 *Activity Diagram*

Activity Diagram adalah salah satu jenis diagram dalam Unified Modeling Language (UML) yang digunakan untuk menggambarkan alur kerja atau urutan langkah-langkah dalam suatu sistem, proses bisnis, atau algoritma.

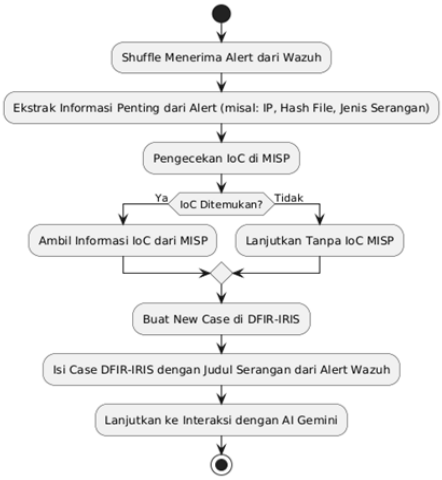
Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

a. *Activity Diagram* Pengiriman Alert Wazuh



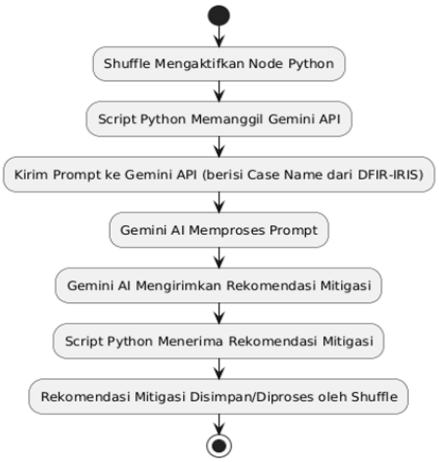
Gambar 3. *Activity Diagram* Pengiriman Alert Wazuh

b. *Activity Diagram* Pemrosesan *Alert* di *Shuffle*



Gambar 4. *Activity Diagram* Pemrosesan *Alert Shuffle*

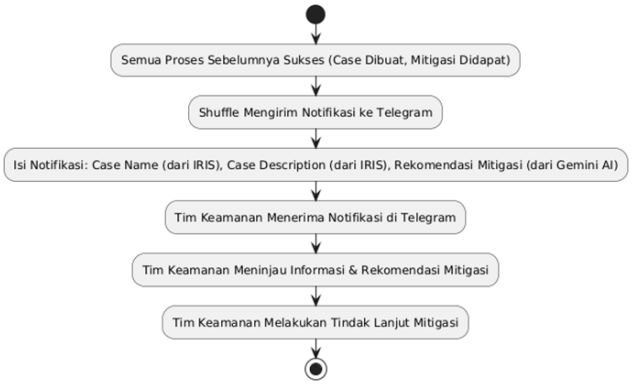
c. *Activity Diagram* Interaksi dengan AI Gemini



Gambar 5. *Activity Diagram* Interaksi AI Gemini

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

d. *Activity Diagram* Notifikasi ke Tim Keamanan

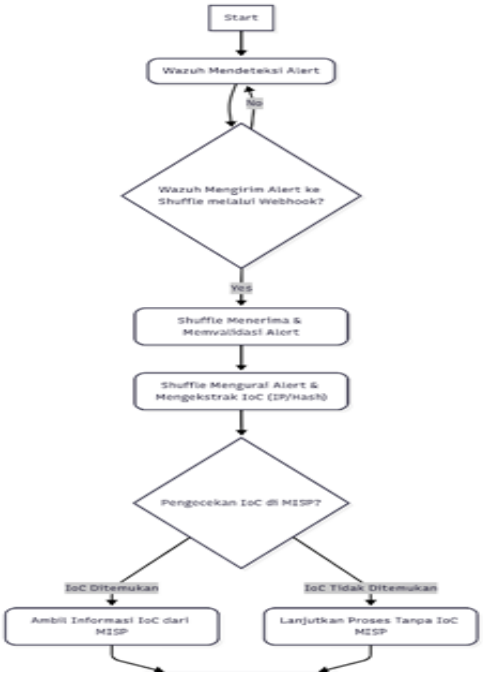


Gambar 6. *Activity Diagram* Notifikasi ke Tim Keamanan

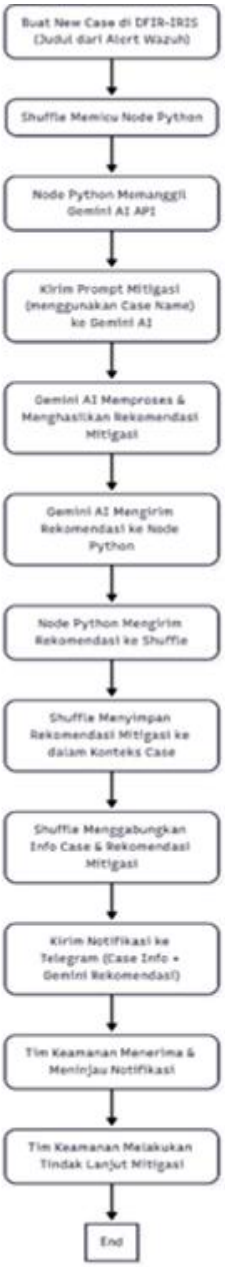
Gambar di atas adalah diagram aktivitas yang menunjukkan alur proses otomatisasi respons terhadap insiden keamanan siber. Diagram ini melibatkan beberapa pihak dan komponen sistem, yaitu Sistem Wazuh, Shuffle SOAR (sebagai orkestrator), MISP, DFIR-IRIS, AI Gemini, Telegram, dan Tim Keamanan, masing-masing memiliki peran dalam alur kerja tersebut. Proses dimulai ketika Sistem Wazuh mendeteksi ancaman keamanan dan mengirimkan peringatan ke Shuffle SOAR. Setelah itu, Shuffle menerima dan memproses peringatan tersebut, lalu memperkaya data dengan mencari bukti indikasi ancaman (IoC) di MISP dan membuat laporan insiden di DFIR-IRIS. Kemudian, AI Gemini dipanggil untuk memberikan rekomendasi mitigasi, yang selanjutnya digabung dalam notifikasi lengkap dan dikirimkan ke Telegram. Sebagai langkah terakhir, Tim Keamanan menerima notifikasi tersebut dan dapat mengakses detail laporan insiden di DFIR-IRIS untuk mengevaluasi rekomendasi serta mengambil tindakan sebelum proses selesai.

3.2.3 *Flowchart*

Flowchart adalah gambar grafis yang menunjukkan langkah-langkah dan urutan prosedur dalam sebuah program. Flowchart membantu analis dan programmer memecah masalah menjadi bagian-bagian yang lebih kecil serta mendukung dalam menganalisis berbagai pilihan alternatif dalam proses pengoperasian [7].



Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376



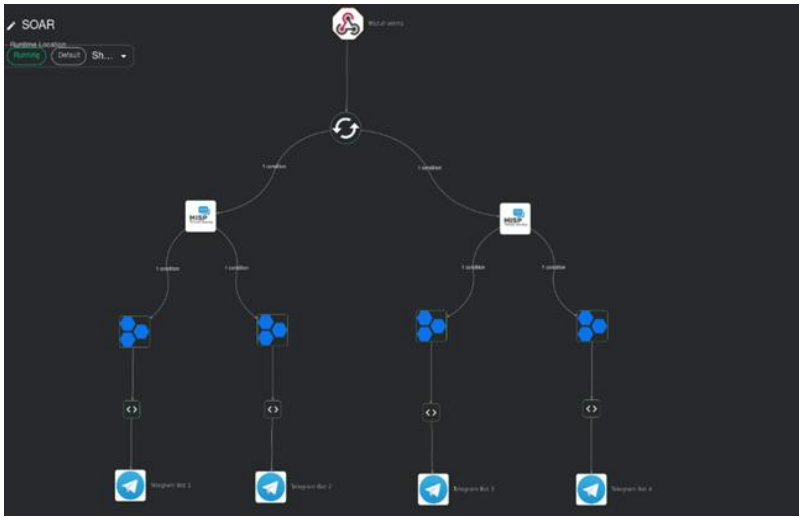
Gambar 7. *Flowchart*

3.3 Implementasi

a. Tampilan Rancangan Layar Alur Kerja Utama di Shuffle

Layar ini menunjukkan berbagai node yang masing-masing mewakili komponen dan langkah-langkah dalam proses otomatisasi, saling terhubung untuk membentuk alur respons insiden yang jelas dan konsisten. Setiap node memiliki fungsi tertentu, seperti mengaktifkan peringatan dari Wazuh, modul untuk mendekode dan memparsing data, integrasi dengan platform intelijen ancaman (MISP), sistem manajemen kasus (DFIR-IRIS), mesin rekomendasi berbasis AI (Gemini), hingga saluran pengiriman notifikasi (Telegram). Tampilan ini langsung mencerminkan struktur dan logika proses yang telah dijelaskan dalam diagram sebelumnya, sehingga memudahkan desainer dan pengelola sistem dalam membangun, mengvisualisasikan, serta mengelola otomatisasi secara lebih mudah.

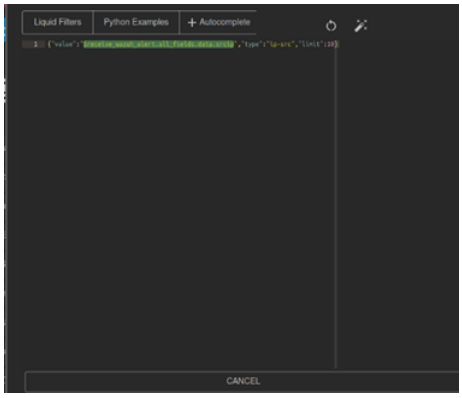
Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376



Gambar 8. *Workflow* SOAR

b. Tampilan Rancangan Layar Konfigurasi Integrasi MISP

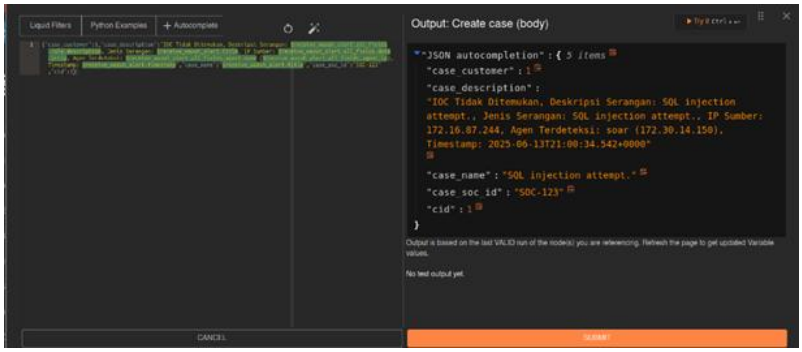
Layar ini menampilkan antarmuka konfigurasi node MISP di Shuffle, yang merupakan tempat desainer sistem menentukan parameter pencarian Indikator Kompromi (IoC).



Gambar 9. Tampilan Misp IoC

c. Tampilan Rancangan Layar Konfigurasi Integrasi DFIR-IRIS

Layar ini menampilkan antarmuka konfigurasi node DFIR-IRIS di Shuffle, tempat desainer sistem mendefinisikan bagaimana data dari alert keamanan yang masuk akan dipetakan ke dalam field-field kasus insiden di platform DFIR-IRIS.

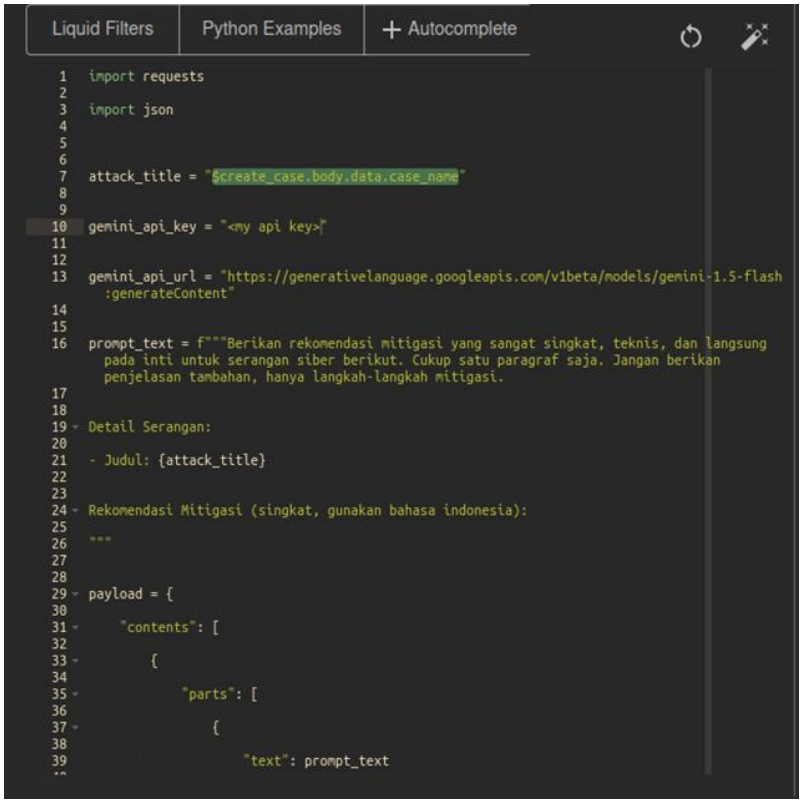


Gambar 10. Tampilan Konfigurasi DFIR-IRIS

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

d. Tampilan Rancangan Layar Konfigurasi Node Python (Logika Pemrosesan Data dan Interaksi AI)

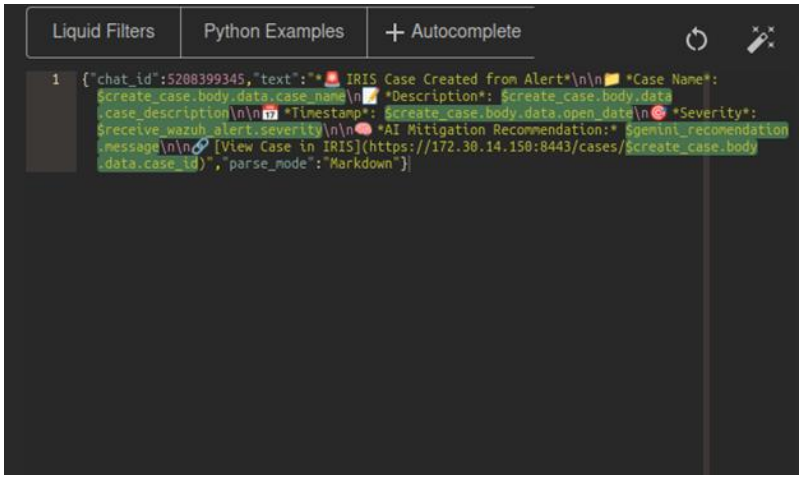
Layar ini menampilkan antarmuka konfigurasi Node "Execute Python Script" di Shuffle, tempat kode Python dirancang. Kode ini berfungsi untuk menerima dan mem-parsing data alert, serta secara spesifik mengambil case_name dari kasus DFIR-IRIS (yang merupakan judul serangan Wazuh).



Gambar 11. Tampilan Konfigurasi AI Gemini

e. Tampilan Rancangan Layar Konfigurasi Notifikasi Telegram

Layar ini menampilkan antarmuka konfigurasi Node Telegram Bot di Shuffle, tempat desainer sistem menyusun konten dan format pesan notifikasi insiden.



Gambar 12. Tampilan Konfigurasi Telegram

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 2, Juli 2025
ISSN 3024-8248 (media online)
Hal 368-376

4. KESIMPULAN

Setelah uji coba dilakukan terhadap pembangunan dan penerapan Sistem Security Orchestration, Automation, and Response (SOAR) di Universitas Terbuka, maka dapat diambil kesimpulan. Sistem SOAR ini dikembangkan khusus untuk kebutuhan Universitas Terbuka dan diharapkan mampu memberikan solusi yang efektif dan efisien bagi tim keamanan dalam proses deteksi, triase, serta tanggapan terhadap kejadian serangan siber.

Sistem ini tidak hanya akan memudahkan tim keamanan dalam mengelola alert dan kasus insiden, tetapi juga akan membantu manajemen dalam memantau dan menganalisis data ancaman serta respons secara lebih efektif, sehingga pada akhirnya meningkatkan efisiensi operasional keamanan dan kekuatan pertahanan siber universitas secara keseluruhan. Dengan mengintegrasikan AI Gemini ke dalam sistem ini, universitas akan mengalami perubahan positif dalam cara mengelola dan menerapkan rekomendasi mitigasi, karena akan diberikan panduan yang lebih cepat, akurat, dan tepat sasaran dibandingkan dengan proses penanganan insiden yang sebelumnya masih terbatas. Kesimpulan ini menjelaskan langkah-langkah yang perlu diambil agar sistem SOAR yang dikembangkan dapat memenuhi kebutuhan tim keamanan dan manajemen universitas secara efektif.

REFERENCES

Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, “Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia,” *J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 1135–1145, 2023.

P. Ananda Khairunnisa *et al.*, “Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia,” *J. Ilmu Tek. dan Inform.*, vol. 4, pp. 9–16, 2024.

A. Shafiyyah, G. F. Nama, and R. A. Pradipta, “Implementasi Wazuh Menggunakan Metode Ppdioo Di Sistem Keamanan Jaringan Psdku Universitas Lampung Waykanan Sebagai Deteksi Dan Respon Serangan Siber,” *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 2, 2024, doi: 10.23960/jitet.v12i2.4074.

D. Meisak, Hendri, and S. R. Agustini, “Penerapan Metode Prototype Pada Perancangan Sistem Informasi Penjualan Mediatama Solusindo Jambi,” *STORAGE J. Ilm. Tek. dan Ilmu Komput.*, vol. 1, no. 4, pp. 1–11, 2022, doi: 10.55123/storage.v1i4.1066.

K. Kurniati, “Penerapan Metode Prototype Pada Perancangan Sistem Pengarsipan Dokumen Kantor Kecamatan Lais,” *J. Softw. Eng. Ampera*, vol. 2, no. 1, pp. 16–27, 2021, doi: 10.51519/journalsea.v2i1.89.

K. Nistrina and L. Sahidah, “Unified Modelling Language (Uml) Untuk Perancangan Sistem Informasi Penerimaan Siswa Baru Di Smk Marga Insan Kamil,” *J. Sist. Informasi, J-SIKA*, vol. 4, no. 1, p. 17, 2022.

A. Zalukhu, P. Swingly, and D. Darma, “Perangkat Lunak Aplikasi Pembelajaran Flowchart,” *J. Teknol. Inf. dan Ind.*, vol. 4, no. 1, pp. 61–70, 2023, [Online]. Available: https://ejurnal.istp.ac.id/index.php/jtii/article/view/351