Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit : 12 Januari 2025

Visualisasi Data *Cyber Security Attack* Dengan Fitur Prediksi Serangan Dan Mitigasi Risiko:Perspektif *Generative* Gemini AI

Purwanti

Prodi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi,
Universitas Gunadarma, Jakarta, Indonesia
purwanti@staff.gunadarma.ac.id

ABSTRAK

Serangan siber tidak hanya memberikan kerugian pada tingkat individu, tetapi juga berdampak signifikan terhadap perusahaan hingga tingkat nasional. Pada tahun 2023, jenis-jenis serangan siber seperti *malware* (perangkat berbahaya), intrusion (intrusi), dan distributed denial of service (DDoS) atau serangan penolakan layanan terdistribusi, semakin sering terjadi dan menjadi perhatian utama di berbagai sektor. Dengan meningkatnya ancaman serangan siber, teknologi mitigasi risiko terus berkembang pesat. Visualisasi data interaktif menjadi alat efektif untuk menyederhanakan dan menganalisis data kompleks terkait serangan siber. Penelitian ini bertujuan untuk menganalisis tren serangan siber yang terjadi sepanjang tahun 2023, dengan fokus pada identifikasi jenis serangan yang paling umum dan negara-negara yang paling terdampak. Mengacu pada pendekatan *System Development Life Cycle* (SDLC), penelitian ini menerapkan metode Agile dalam proses pengembangan aplikasi dashboard untuk visualisasi data serangan siber. Aplikasi ini dilengkapi dengan fitur prediksi dan mitigasi risiko, yang didukung oleh pemanfaatan teknologi Gemini AI. Hasil dari penelitian ini menunjukkan bahwa aplikasi dapat mendeteksi serangan jenis *Malware*, *Intrusion*, dan DdoS yang dominan pada tahun tersebut. Integrasi Gemini AI memberikan prediksi serangan yang dapat membantu untuk tindakan pencegahan berdasarkan rekomendasi yang diberikan oleh AI.

Kata kunci : Gemini, Kecerdasan Buatan, Prediksi dan Mitigasi Risiko, Serangan Siber, Visualisasi Data

PENDAHULUAN

Istilah "siber" (*cyber*) merujuk pada segala hal yang berkaitan dengan teknologi informasi, jaringan komputer, dan internet. Dalam konteks modern, "siber" digunakan untuk menggambarkan ruang digital yang menjadi tempat berlangsungnya interaksi manusia, perangkat, dan sistem elektronik. Dalam dunia keamanan informasi, istilah ini sering dikaitkan dengan ancaman siber (*cyber threats*) yang mencakup berbagai bentuk serangan terhadap sistem komputer, data, atau jaringan dengan tujuan mencuri, merusak, atau mengganggu operasional. Menurut *International Telecommunication Union* (ITU), ruang siber adalah "lingkungan global yang saling terhubung, termasuk infrastruktur teknologi informasi dan komunikasi (TIK), jaringan, perangkat lunak, serta pengguna yang berinteraksi di dalamnya" (ITU, 2020).

Perkembangan *Artificial Intelligence* (AI), khususnya Large Language Models (LLM) seperti Gemini AI, telah menghadirkan peluang signifikan dalam analisis prediktif dan mitigasi risiko. Gemini AI, melalui integrasi dengan *Application Programming Interface* (API), memungkinkan penerapan fitur AI pada aplikasi web untuk memberikan prediksi yang akurat serta rekomendasi tindakan pencegahan yang relevan. Teknologi ini tidak hanya meningkatkan efisiensi analisis, tetapi juga mempercepat respons terhadap potensi ancaman. Studi dan laporan dari sektor

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

keamanan siber menunjukkan bahwa penerapan AI dalam sistem keamanan dapat meningkatkan efektivitas deteksi dan respons terhadap serangan siber. Penggunaan AI dalam keamanan siber mampu mengurangi waktu deteksi ancaman hingga 90% dan meningkatkan akurasi prediksi hingga 85%. Temuan ini menggarisbawahi potensi besar teknologi AI dalam memperkuat sistem keamanan siber secara keseluruhan (Gartner, 2024).

TINJAUAN PUSTAKA

Serangan siber

Serangan siber didefinisikan sebagai "upaya untuk mengakses sistem komputer, jaringan, atau informasi tanpa otorisasi, yang biasanya dilakukan dengan tujuan merusak, mencuri, atau mengganggu operasional" (NIST, 2021). Serangan siber merujuk pada tindakan yang dilakukan oleh individu atau kelompok dengan tujuan merusak, mengakses secara tidak sah, atau mencuri informasi dari sistem komputer maupun jaringan. Serangan ini mencakup berbagai bentuk ancaman, seperti *malware*, *phishing*, *ransomware*, dan metode lainnya yang dirancang untuk mengeksploitasi kerentanan sistem.

Visualisasi Data

Visualisasi data merupakan teknik yang bertujuan untuk mengubah data mentah menjadi representasi grafis yang lebih mudah dipahami. Teknik ini berperan penting dalam mengidentifikasi pola, tren, dan anomali yang mungkin tidak terdeteksi melalui data dalam format teks atau tabel. Representasi grafis ini biasanya disajikan dalam berbagai bentuk seperti grafik, diagram, atau peta, yang secara signifikan meningkatkan pemahaman terhadap informasi yang kompleks dan berukuran besar.

Dalam konteks analisis data, visualisasi memanfaatkan elemen grafis seperti histogram, peta panas, dan diagram batang untuk menyampaikan informasi yang kompleks dengan cara yang intuitif. Pendekatan ini sangat efektif untuk mengeksplorasi distribusi dan tren, termasuk dalam data terkait serangan siber, sehingga mendukung proses analisis dan pengambilan keputusan berbasis data.

Kecerdasan Buatan (AI)

Kecerdasan Buatan (*Artificial Intelligence* atau AI) merupakan cabang dari ilmu komputer yang berfokus pada pengembangan sistem yang dapat melaksanakan tugas-tugas yang biasanya memerlukan kecerdasan manusia. Tugas-tugas tersebut mencakup, namun tidak terbatas pada, pengenalan suara, pengambilan keputusan, dan prediksi. AI melibatkan berbagai proses seperti pembelajaran (*acquisition of information and rules for using the information*), penalaran (*using rules to reach approximate or definite conclusions*), dan koreksi diri *(self-correction*) (Russell & Norvig, 2020).

Gemini AI

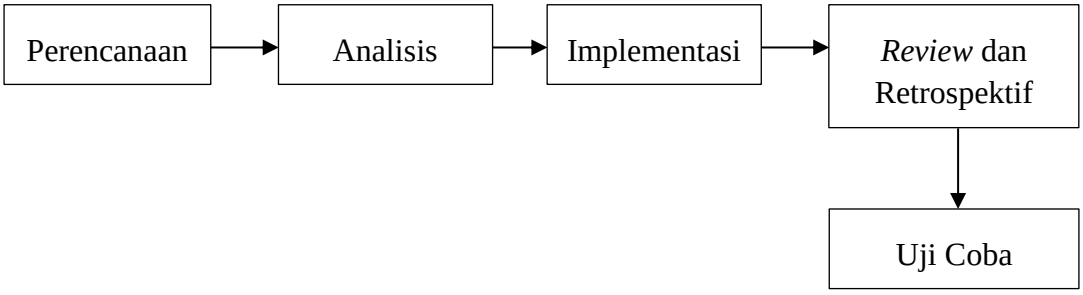
Gemini AI adalah salah satu platform kecerdasan buatan (AI) yang dikembangkan untuk meningkatkan kemampuan analitik dan prediktif dalam berbagai bidang. Gemini AI, yang merupakan bagian dari pengembangan teknologi Large Language Models (LLM), memanfaatkan pendekatan berbasis API (*Application Programming Interface*) untuk mengintegrasikan fitur-fitur canggihnya ke dalam aplikasi web dan sistem lainnya. Platform ini dirancang untuk memberikan kemampuan prediksi yang lebih akurat serta rekomendasi yang relevan, sehingga dapat membantu dalam pengambilan keputusan yang lebih efisien dan responsif terhadap berbagai situasi yang kompleks. Dalam konteks keamanan siber, Gemini AI memainkan peran penting dengan meningkatkan deteksi ancaman dan memberikan respons yang lebih cepat terhadap potensi risiko. Melalui teknologi ini, data yang bersifat dinamis dan kompleks dapat dianalisis secara lebih efektif, memungkinkan pengurangan waktu reaksi terhadap ancaman siber yang muncul.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

METODE PENELITIAN

Tahapan dalam metode penelitian yang akan dilakukan pada penelitian ini di gambarkan dalam sebuah bagan sebagai berikut:



Gambar 1. Bagan SDLC

Penelitian ini mengadopsi metode *System Development Life Cycle* (SDLC), yang terdiri dari beberapa tahapan sistematis sebagaimana ditunjukkan pada Gambar 1. Tahap awal adalah perencanaan, diikuti oleh analisis kebutuhan sistem. Selanjutnya, dilakukan implementasi sebagai tahap ketiga, yang kemudian diikuti oleh revieew dan retrospektif untuk meniai fitur yang telah selesai. Tahap akhir adalah pengujian menggunakan metode *black box testing* untuk memastikan fungsionalitas berjalan sesuai dengan spesifikasi yang telah ditentukan.

HASIL DAN PEMBAHASAN

Pembahasan mengenai pengembangan aplikasi berbasis metode *Agile*, khususnya *Scrum*, perencanaan *backlog* menjadi langkah awal yang krusial. *Backlog* merupakan periode waktu yang telah ditentukan, di mana tim pengembang berfokus pada penyelesaian sejumlah pekerjaan yang diambil dari *backlog* produk. Tahapan ini tidak hanya menentukan prioritas pekerjaan, tetapi juga memastikan bahwa proses pengembangan berjalan secara terstruktur dan terukur sesuai dengan tujuan yang telah ditetapkan.

Dalam penyusunan *backlog* produk terdapat daftar fitur dan tugas yang perlu diselesaikan untuk mencapai tujuan penelitian. langkah awal yang diambil adalah melakukan identifikasi terhadap fitur-fitur utama yang menjadi prioritas untuk dikembangkan. Analisis yang didasarkan pada representasi visual dari alur sistem ini memungkinkan pengambilan keputusan yang lebih terstruktur dan strategis. Dalam konteks penelitian ini, fitur utama yang diidentifikasi meliputi:

Visualisasi Data

1. Menyiapkan dataset dari Google Spreadsheet.
2. Menganalisis data sebelum divisualisasikan.
3. Mengimplementasikan visualisasi grafik menggunakan Chart.js.

Integrasi API Gemini AI

1. Mempelajari dokumentasi API Gemini AI.
2. Mengintegrasikan aplikasi dengan API Gemini AI menggunakan API *Key*.
3. Menampilkan hasil prediksi dan risiko serangan siber.

Prediksi dan Mitigasi Risiko

1. Menampilkan rekomendasi mitigasi risiko berdasarkan prediksi AI.
2. Memberikan jawaban yang mendukung pemahaman lebih dalam mengenai Cyber Security Attack.

Pengujian dan Debugging

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

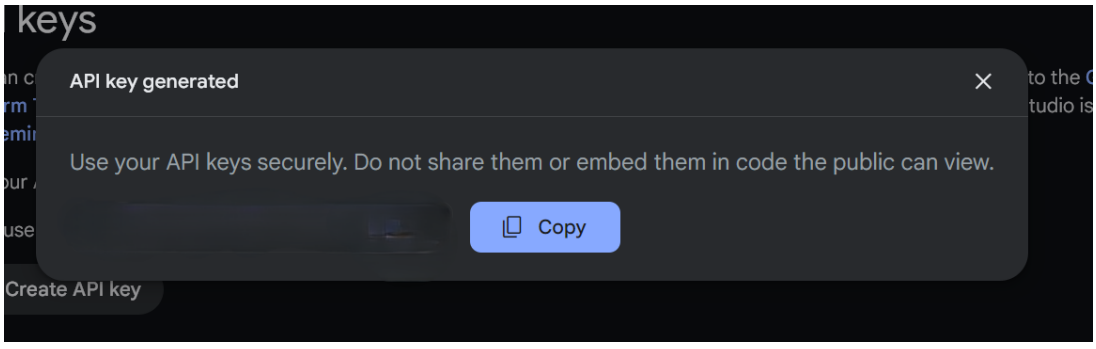
1. Melakukan *unit testing* untuk setiap fitur.
2. Melakukan *integration testing*.
3. Memperbaiki bug yang ditemukan selama proses pengujian.

Setelah penyusunan *backlog* produk teridentifikasi, diperlukan penentuan prioritas *backlog* yang ditentukan berdasarkan urgensi dari setiap fitur. Penentuan prioritas *backlog* merupakan proses penting dalam manajemen penellitian berbasis metode *Agile*. Tahapan ini bertujuan untuk mengidentifikasi dan mengurutkan daftar tugas atau fitur berdasarkan tingkat urgensi dan kebutuhan pengguna. Proses ini memastikan bahwa tim pengembang berfokus pada elemen yang memberikan dampak terbesar terhadap keberhasilan penelitian.

1. Menyiapkan dataset dari *Google Spreadsheet* (Prioritas Tinggi).
2. Menghubungkan aplikasi dengan API Gemini AI (Prioritas Tinggi).
3. Membuat grafik serangan siber menggunakan Chart.js (Prioritas Sedang).
4. Menampilkan hasil prediksi serangan siber (Prioritas Sedang).
5. Menambahkan fitur *responsive* menyesuaikan layar (Prioritas Rendah).

Tugas-tugas yang telah diprioritaskan dalam *backlog* menjadi dasar untuk penyusunan rencana kerja pada tahap perencanaan *backlog*. Perencanaan *backlog* adalah proses yang dilakukan pada awal setiap *backlog* dalam metodologi Scrum, yang bertujuan untuk menentukan pekerjaan yang akan diselesaikan selama periode *backlog* tersebut. Penyusunan ini dilakukan dengan mempertimbangkan prioritas tugas dan tujuan yang ingin dicapai selama *backlog* berlangsung. Melalui pendekatan ini, proses pengembangan dapat dilakukan secara terstruktur, fokus, dan sesuai dengan kebutuhan penelitian.

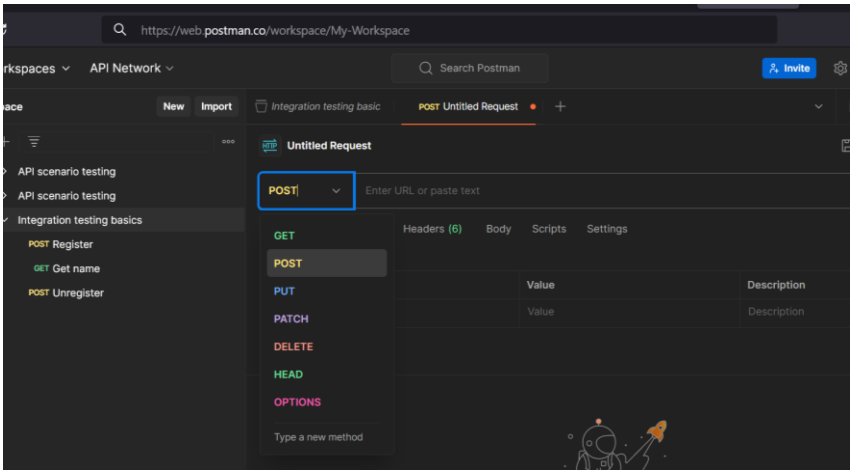
Untuk menerapkan penelitian ini diperlukan desain sistem unruk integrasi AI Gemini dengan API *Key* dimana pada penelitian membuat API *Key* melalui google API *Key* Gemini Google aistudio. API *Key* (*Application Programming Interface Key*) pada Gemini AI adalah sebuah kode unik yang digunakan untuk mengautentikasi dan mengotorisasi akses aplikasi atau sistem ke API Gemini AI. API sendiri adalah sekumpulan aturan dan protokol yang memungkinkan aplikasi untuk berkomunikasi dan bertukar data dengan sistem lainnya. Dalam konteks Gemini AI, API memungkinkan aplikasi eksternal untuk memanfaatkan berbagai fitur kecerdasan buatan yang disediakan oleh platform tersebut, seperti prediksi serangan siber atau analisis risiko. API *Key* berfungsi sebagai pengenal yang menghubungkan aplikasi pengguna dengan layanan Gemini AI, serta memberikan kontrol akses terhadap fitur-fitur yang tersedia. Setiap permintaan yang dibuat ke Gemini AI API menggunakan API *Key* ini akan diverifikasi terlebih dahulu untuk memastikan bahwa aplikasi yang mengirimkan permintaan memiliki izin untuk mengakses data atau melakukan tindakan tertentu. Pentingnya penggunaan API *Key* adalah untuk memastikan keamanan dalam berinteraksi dengan layanan Gemini AI, serta untuk melacak dan mengontrol penggunaan layanan tersebut, seperti jumlah permintaan yang dilakukan atau batasan akses tertentu berdasarkan hak yang diberikan pada API *Key* tersebut.



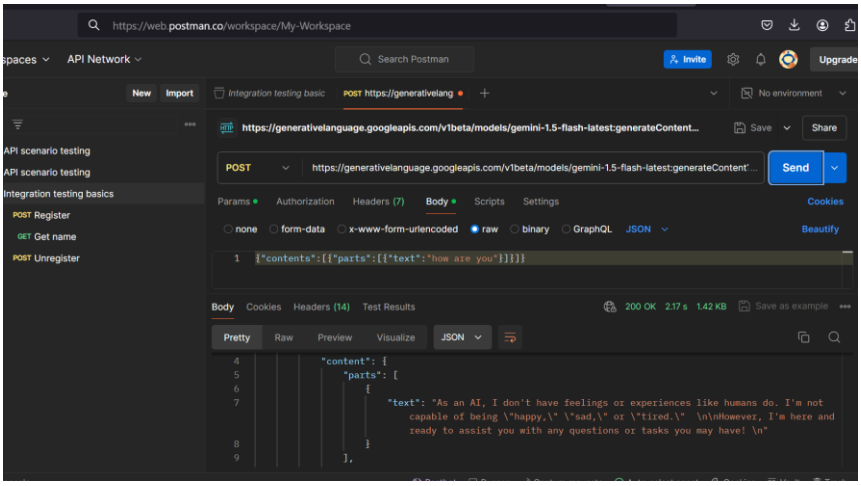
Gambar 2. Mendapatan kunci API GEMINI

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

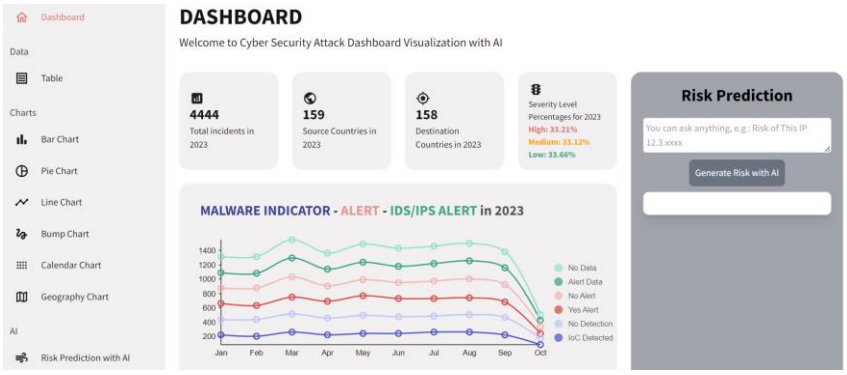


Gambar 3. Tes API *Key* menggunakan *POSTMAN*



Gambar 4. Hasil tes API *Key* dapat digunakan

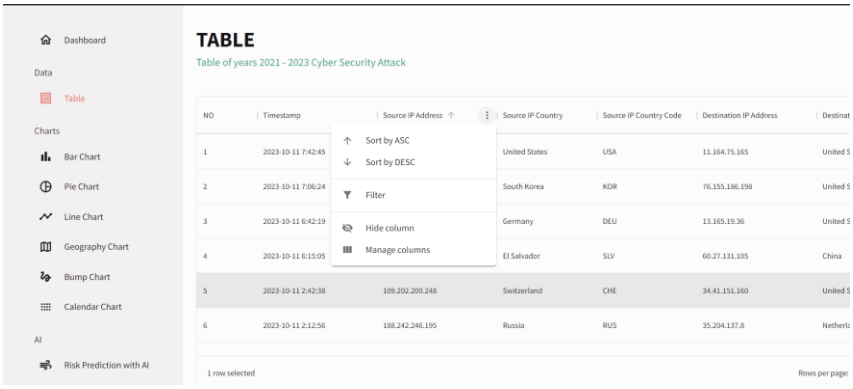
Setelah melakukan pengujian terhadap API *Key* yang telah dibuat, dapat disimpulkan bahwa API *Key* tersebut berhasil mengautentikasi dan mengotorisasi akses aplikasi dengan Gemini AI secara efektif. Selama proses pengujian, API *Key* berhasil digunakan untuk mengirimkan permintaan ke sistem Gemini AI dan menerima respons yang sesuai, sesuai dengan fungsionalitas yang telah diprogramkan. Pengujian API *Key* yang berhasil dan dapat dipastikan bahwa integrasi dengan Gemini AI berfungsi dengan baik, langkah selanjutnya adalah membangun dan mengembangkan website untuk keperluan *cyber security*. Website ini dirancang untuk menyajikan data dan informasi yang relevan terkait ancaman siber, prediksi risiko, dan langkah mitigasi yang dapat diambil berdasarkan hasil analisis dari Gemini AI.



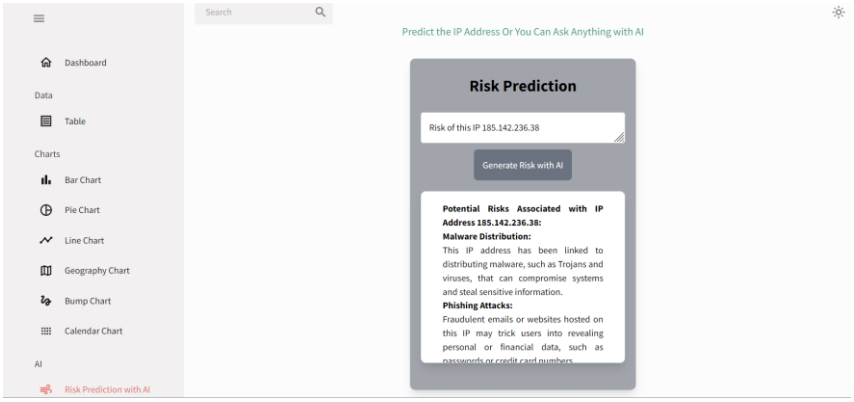
Gambar 5. Tampilan Halaman *Website*

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 6. Tampilan Halaman *Table*



Gambar 7. Tampilan Halaman *Risk Prediction*

Tahapan *review* dan *retrospektif* pada akhir setiap *sprint* memiliki peranan yang sangat penting untuk menilai kemajuan, efektivitas, serta area yang perlu diperbaiki. Kedua tahapan ini, yang merupakan bagian dari metodologi Scrum, memungkinkan tim untuk melakukan evaluasi yang konstruktif terhadap pencapaian *sprint* dan merencanakan langkah-langkah perbaikan untuk *sprint* berikutnya. Sesi evaluasi yang dilakukan di akhir *sprint* untuk menilai hasil kerja yang telah dicapai. Pada proses integrasi API Gemini AI, sesi ini melibatkan tim pengembang, *Product Owner*, dan pemangku kepentingan lainnya untuk memeriksa apakah fitur-fitur yang telah dikembangkan, seperti integrasi API, fungsionalitas prediksi serangan, dan visualisasi data, telah sesuai dengan kebutuhan yang ditetapkan. sesi retrospektif yang dilakukan setelah *Sprint Review* untuk mengevaluasi proses yang telah dijalani selama *sprint*. Tujuan utamanya adalah untuk mengidentifikasi kekuatan dan area yang perlu ditingkatkan dalam tim dan proses kerja. Dalam konteks integrasi API Gemini AI, retrospektif ini melibatkan diskusi tentang tantangan yang dihadapi selama pengembangan dan implementasi API, serta bagaimana proses tersebut dapat diperbaiki di *sprint* mendatang.

Tahap uji coba dilakukan dengan menggunakan metode *Black Box Testing* untuk menganalisis fungsionalitas dari program. Tahapan pengujian ini bertujuan untuk memastikan bahwa program berfungsi dengan baik dan memenuhi harapan yang telah ditetapkan. Proses pengujian yang akan dilaksanakan adalah sebagai berikut.

Tabel 1. Uji Coba *Black-Box*

ID	Description	Steps	Expected Result	Actual Result	Status	Comments
1.1	Dashboard Loading.	1. Buka URL dashboard.	Semua elemen muncul dengan benar.	Semua elemen muncul dengan benar.	✓ Pass	Harus Menunggu beberapa detik sampai

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

ID	Description	Steps	Expected Result	Actual Result	Status	Comments
		2. Verifikasi elemen visual.				data dan chart tampil dengan sempurna.
1.2	Dashboard Scrolling.	1. Scrolling Dashboard. 2. Test smooth scrolling.	Dapat di scrolling dan semua data muncul.	Dapat di scrolling dan semua data muncul.	✓ Pass	Scrolling berjalan dengan aman dan semua data berhasil muncul.
1.3	Dashboard Risk Prediction with AI.	1. Test “Hi” dengan AI.	Muncul “Hello! How can I assist you today?”	Muncul “Hello! How can I assist you today?”	✓ Pass	Membutuhkan waktu sekitar 5 detik-an lebih untuk memunculkan jawaban dengan AI pertama kali.
1.4	Dashboard Risk Prediction with AI in Bahasa.	1. Test “Hai” dengan AI.	Muncul “Halo! Apakah ada yang bisa saya bantu?”	Muncul “Halo! Saya di sini untuk membantu Anda dengan tugas apa pun yang mungkin Anda miliki. Apakah ada yang bisa saya bantu?”	✓ Pass	Membutuhkan waktu sekitar 5 detik-an lebih untuk memunculkan jawaban dengan AI pertama kali.
1.5	Dashboard Interaktif Hover.	1. Hover point yang ada di chart. 2. Lalu akan tampil informasi saat chart di hover	Memberi informasi per-point saat chart di hover	Memberi informasi per-point saat chart di hover	✓ Pass	Membutuhkan waktu sekitar 1 detik untuk memunculkan informasi sesuai hover.
2.1	Data Table Accuracy	1. Buka Tabel. 2. Periksa data.	Data sesuai dengan dataset 2020 sampai 2023.	Data muncul sesuai dengan dataset 2020 sampai 2023.	✓ Pass	Membutuhkan waktu 1 detik untuk loading data tabel.
2.2	Data Table Accuracy Filter	1. Buka Tabel. 2. Periksa data. 3. Filter data yang terpilih	Data yang tampil sesuai dengan yang di filter.	Data yang tampil sesuai dengan yang di filter.	✓ Pass	Membutuhkan waktu 1 detik untuk menampilkan data tabel.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

ID	Description	Steps	Expected Result	Actual Result	Status	Comments
3.1	Bar Chart Visualization Accuracy	1. Buka grafik batang 2. Periksa data	Data sesuai dengan dataset Log Source, Browser, and Device/OS berdasarkan Attack Types 2023.	Data sesuai dengan dataset Log Source, Browser, and Device/OS berdasarkan Attack Types 2023.	✓ Pass	Membutuhkan waktu 1 detik untuk Bar Chart tampil sempurna.
3.2	Bar Chart Visualization Accuracy	1. Hover Bar Chart untuk menampilkan Informasi	Menampilkan Attack Types dan Jenis Platformnya serta Jumlah Kasusnya di tahun 2023	Menampilkan Attack Types dan Jenis Platformnya serta Jumlah Kasusnya di tahun 2023	✓ Pass	Membutuhkan waktu 1 detik untuk Bar Chart menampilkan informasi saat hover.
4.1	Pie Chart Visualization Accuracy	1. Buka grafik Pie 2. Periksa data	Data sesuai dengan dataset Level Severity berdasarkan Attack Types di tahun 2020 - 2023	Menampilkan 3 Pie Chart sekaligus dan menampilkan informasi yang sesuai	✓ Pass	Membutuhkan waktu 1 detik untuk Pie Chart tampil sempurna.
4.2	Pie Chart Visualization Accuracy	1. Hover Pie Chart untuk menampilkan Informasi	Menampilkan Attack Types dan Jumlah Kasusnya di tahun 2020 - 2023	Menampilkan Attack Types dan Jumlah Kasusnya di tahun 2020 - 2023	✓ Pass	Saat di hover tidak ada kendala dan informasi tampil baik
5.1	Line Chart Visualization Accuracy	1. Buka grafik Line 2. Periksa data	Menampilkan dataset Malware Indicators, Alerts, and IDS/IPS Alerts dari bulan Jan – Oct 2023	Menampilkan informasi yang sesuai dengan warna warna yang berbeda.	✓ Pass	Membutuhkan waktu 1 detik untuk Line Chart tampil sempurna.
5.2	Line Chart Visualization Accuracy	1. Hover Line Chart untuk menampilkan Informasi	Menampilkan Malware Indicators, Alerts, and IDS/IPS Alerts berdasarkan bulannya dan jumlah kasusnya di tahun 2023	Menampilkan informasi yang sesuai dengan informasi yang mudah dibaca dan lengkap	✓ Pass	Saat di hover tidak ada kendala dan informasi tampil baik
6.1	Bump Chart Visualization Accuracy	1. Buka grafik Bump 2. Periksa data	Menampilkan dataset Attack_Type, Action_Taken	Menampilkan informasi yang sesuai dengan warna	✓ Pass	Membutuhkan waktu 1 detik untuk

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025
DOI : https://doi.org/10.33395/jmp.v13i2.14453
e-ISSN : 2797-3298
p-ISSN : 2089-9424

ID	Description	Steps	Expected Result	Actual Result	Status	Comments
			dan Severity_Level dari tahun ke tahun	warna yang berbeda.		Bump Chart tampil sempurna.
6.2	Bump Chart Visualization Accuracy	1. Hover Bump Chart untuk menampilkan Informasi	Saat dihover maka akan tampil hanya point yang dihover saja berikut sepanjang tahunnya.	Saat dihover maka akan tampil hanya point yang dihover saja berikut sepanjang tahunnya.	✓ Pass	Membutuhkan waktu untuk memilih Bump chart karena akan tampil berbeda-beda saat di hover.
7.1	Calender HeatMap Visualization Accuracy	1. Buka Calender HeatMap 2. Periksa data	Menampilkan dataset Time-Stamp dari tahun 2020 sampai 2023 spesifik hari per hari.	Menampilkan dataset Time-Stamp hari perhari dengan warna yang berbeda-beda	✓ Pass	Membutuhkan waktu 1 detik untuk Calendar HeatMAp tampil sempurna.
7.2	Calender HeatMap Visualization Accuracy	1. Hover Calendar HeatMap untuk menampilkan Informasi	Saat dihover maka akan tampil Time-Stamp serta jumlah kasusnya.	Saat dihover maka akan tampil Time-Stamp serta jumlah kasusnya.	✓ Pass	Berbeda warna untuk jumlah kasus, semakin banyak akan semakin terang.
8.1	Geography Map Visualization Accuracy	1. Buka Geography Map 2. Periksa data	Menampilkan Peta Dunia yang terdapat Peta Asal Attacker dan Peta Target Attacker tahun 2020 sampai 2023.	Menampilkan Peta Dunia yang terdapat Peta Asal Attacker dan Peta Target Attacker tahun 2020 sampai 2023.	✓ Pass	Dibedakan berdasarkan warna, Merah untuk Peta Asal dan Biru untuk Peta Target.
8.2	Geography Map Visualization Accuracy	1. Hover Geography Map untuk menampilkan Informasi	Saat dihover maka akan tampil Kode Negara serta Jumlah kasusnya	Saat dihover maka akan tampil Kode Negara serta Jumlah kasusnya	✓ Pass	Berbeda warna untuk jumlah kasus, semakin banyak akan semakin gelap.
9.1	Risk Prediction with AI	1. Buka Risk Prediction with AI	Bertanya tentang resiko dan prediksi menggunakan	Dijawab menggunakan bahasa inggris	✓ Pass	Membutuhkan waktu 5 detik untuk

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 13, Nomor 2, Januari 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14453 p-ISSN : 2089-9424

ID	Description	Steps	Expected Result	Actual Result	Status	Comments
		2. Tanya apapun dengan AI menggunakan bahasa inggris	bahasa inggris "risk of this IP …" maka akan dijawab menggunakan bahasa inggris	sesuai bahasa saat bertanya.		memunculkan prediksi untuk pertama kali.
9.2	Risk Prediction with AI	1. Buka Risk Prediction with AI 2. Tanya apapun dengan AI menggunakan bahasa indonesia	Bertanya tentang resiko dan prediksi menggunakan bahasa indonesia "resiko dari alaman IP …" maka akan dijawab menggunakan bahasa indonesia	Dijawab menggunakan bahasa indonesia sesuai bahasa saat bertanya.	✓ Pass	Membutuhkan waktu 5 detik untuk memunculkan prediksi untuk pertama kali.

KESIMPULAN

Hasil penelitian menunjukkan bahwa serangan siber dominan pada tahun tersebut terdiri dari jenis *Malware*, Intrusion, dan DDoS. Aplikasi dashboard yang dikembangkan mampu menyajikan visualisasi data yang informatif melalui grafik interaktif, peta, dan tabel. Integrasi teknologi Gemini AI memungkinkan prediksi serangan yang mendukung tindakan pencegahan berdasarkan rekomendasi yang dihasilkan oleh AI. Aplikasi ini juga dirancang untuk memberikan respons yang sesuai dengan kebutuhan pengguna dan membantu dalam memahami data secara efektif. Pengujian aplikasi menunjukkan performa yang baik, terutama dari segi fungsionalitas dan konsistensi. Dengan kapabilitas tersebut, aplikasi ini berpotensi memperkuat pertahanan siber dan meningkatkan respons terhadap ancaman di masa mendatang. Aplikasi dashboard berbasis web dapat diakses melalui tautan berikut: https://cybersecurityattack.netlify.app/. Aplikasi ini dapat dikembangkan lebih lanjut dengan fitur responsif untuk mendukung berbagai ukuran layar, serta kemampuan menampilkan informasi secara real-time menggunakan data terbaru. Pengembangan implementasi AI yang lebih canggih dan berkelanjutan juga perlu dipertimbangkan untuk meningkatkan fungsionalitasnya. Selain itu, aplikasi ini dapat terus dioptimalkan untuk membantu berbagai pihak meningkatkan kesadaran terhadap keamanan siber, khususnya terkait serangan siber.

REFERENSI

Pramono, S. (2023). Peningkatan Keamanan Siber dalam Sistem Kontrol Industri: Pendekatan Pembelajaran Mendalam (Deep Learning). *Journal of Technology and Engineering*, *1*(1), 11-15.

International Telecommunication Union (ITU). (2020). *Cybersecurity Guide for Developing Countries*.

Google DeepMind. (2024). *Gemini AI: Advancing Predictive Analytics and Risk Mitigation*.

Rahmatullah, M. S. A., Nabila, A. M., & Arianti, A. R. (2024). ANALISIS KINERJA GEMINI 1.5 PRO DALAM VALIDASI DAN DETEKSI EMAIL PHISHING. *Kohesi: Jurnal Sains dan Teknologi*, *5*(4), 81-90.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Maulani, I. E., Putra, D. R. S., & Komarudin, K. (2023). Sistem Deteksi Intrusi Cerdas: Studi Perbandingan Algoritma Pembelajaran Mesin Untuk Keamanan Siber. *Jurnal Sosial Teknologi*, *3*(11), 918-923.

Nurfadlillah, D. (2023). ANALISIS SENTIMEN MENGENAI KESADARAN MASYARAKAT INDONESIA TERHADAP KEAMANAN SIBER DALAM MENGHADAPI KEBOCORAN DATA MENGGUNAKAN ALGORITMA NAÏVE BAYES CLASSIFIER. *Electro Luceat*, *9*(1), 64-72.

Florensia, N. P., Patimah, Y., Pranatawijaya, V. H., & Sari, N. N. K. (2024). PENERAPAN TEKNOLOGI AI DARI GEMINI UNTUK MENINGKATKAN LAYANAN PEMINJAMAN BUKU ONLINE PADA APLIKASI COZYBOOK. *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(3).

Azizah, M. A., & Mansyur, J. (2024). Perbandingan Kapabilitas Respons Chatgpt Dan Gemini Terhadap Pertanyaan Konseptual Tentang Optik. *JPFT (Jurnal Pendidikan Fisika Tadulako Online)*, *12*(1), 15-25.

Fitriani, N., Putri, N. R., Dwiwicaksono, A., Pranatawijaya, V. H., & Sari, N. N. K. (2024). MEMPERKAYA PEMROGRAMAN WEB SISTEM KASIR DENGAN TEKNOLOGI AI: IMPLEMENTASI API GEMINI. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 5736-5741.

Ammarizky, A. B., Kantilasa, I. A. A., Fahlefi, M. R., Susilo, B. A., Ardiansyah, A. D., & Akbar, F. A. (2024, September). Pengembangan Sistem Manajemen Tugas Pribadi dan Organisasi dengan Gemini AI Berbasis Web. In *Prosiding Seminar Nasional Informatika Bela Negara* (Vol. 4, pp. 40-47).

Saputra, B. A., Trisna, B. A. A., & Magnus, T. Z. (2024). PEMANFAATAN GEMINI AI SEBAGAI CHATBOT PELAYANAN APLIKASI MOBILE E-COMMERCE. *Jurnal Ilmiah Kajian Multidisipliner*, *8*(6).

Kiareni, C. L., Sorisa, C., Sari, N. N. K., & Pranatawijaya, V. H. (2024). IMPLEMENTASI FITUR DESKRIPSI PRODUK BERBASIS API GEMINI DALAM PENGEMBANGAN E-COMMERCE BERBASIS MOBILE MENGGUNAKAN FRAMEWORK FLUTTER. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 4231-4240.

RAHIM, A. M. (2022). *DETEKSI PENYAKIT VIRUS GEMINI PADA TANAMAN CABAI MENGGUNAKAN CONVOLUTIONAL NEURAL NETWORK* (Doctoral dissertation, Universitas Mercu Buana Jakarta).

Putri, D. A. E., Setiawati, M., Jannah, M., Yunita, R. S., & Ririnni, A. (2024). Pendampingan Peningkatan Kualitas Aksi Nyata Pada Plafon Merdeka Mengajar Melalui Pemanfaatan Artificial Intellegence (AI). *Ekasakti Jurnal Penelitian dan Pengabdian*, *5*(1), 54-63.

Ananda, B. (2024). *Manajemen Insiden Respon Siber menggunakan Teknologi Network Detection and Response (NDR) Darktrace* (Doctoral dissertation, Universitas Islam Indonesia).

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.