Keamanan Siber

Kelompok 9

Fadil Prasetyo Alfarizzi (123450048)

Reynaldi Rahmad (122450088)

Fathya Intami Gusda (123450095)

Melinza Nabila (123450122)

Business Domain Overview

Domain Bisnis : Manajemen Insiden Keamanan Siber pada Jaringan Organisasi

Aktivitas Utama :

- Deteksi dan monitoring insiden secara real-time
- Klasifikasi jenis serangan (Malware, DDoS, SQL Injection, Phishing)
- Pencatatan server dan unit yang terdampak
- Penanganan insiden oleh tim keamanan
- Pelaporan dan evaluasi kinerja

Permasalahan : Data Insiden tersebar dan sulit dianalisis secara terstruktur

Solusi : Membangun Data Warehouse Kemaanan Siber sebagai pusat data untuk mendukung analisis dan pengambilan keputusan

Project Objectives

Tujuan dari proyek Data Warehouse Keamanan Siber ini adalah:

- Membangun data warehouse terpusat untuk mengelola data insiden keamanan siber
- Mengintegrasikan data dari berbagai sumber ke dalam tabel dimensi dan fakta
- Mendukung analisis jumlah insiden berdasarkan waktu, lokasi, jenis serangan, dan tim respon
- Mengukur kinerja penanganan insiden melalui metrik durasi respon dan status penyelesaian
- Menyediakan dasar data yang akurat untuk dashboard eksekutif, operasional, dan analisis dampak

Requirements & Design

1. Business Requirements
Sistem harus mampu:
- Mengelola data insiden keamanan siber secara terpusat
- Mencatat waktu kejadian, lokasi, jenis serangan, dan tim respon
- Mendukung laporan harian, mingguan, dan bulanan
- Menyediakan data untuk analisis manajemen dan dashboard

Stakeholders utama:
- CISO
- Koordinator Tim Respon Insiden
- Staff Keamanan IT
- Pimpinan Fakultas / Unit TI

2. Key KPIs Identified
KPI yang digunakan:
- Rata-rata durasi respon insiden
- Jumlah insiden per bulan
- Frekuensi serangan per fakultas / unit
- Jumlah data yang terdampak
- Persentase insiden yang diselesaikan tepat waktu

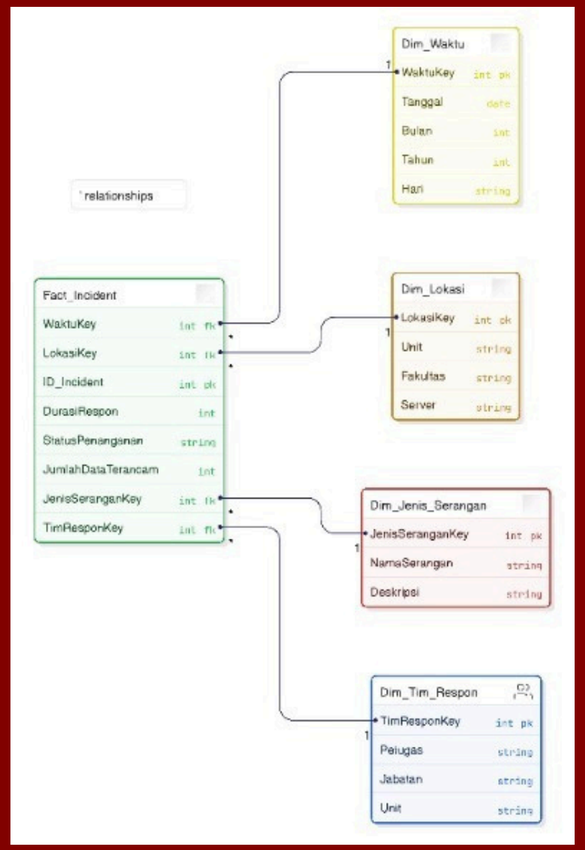


Diagram ERD

Implementation

Database Skema

Database :
DM_KeamananSiber_DW

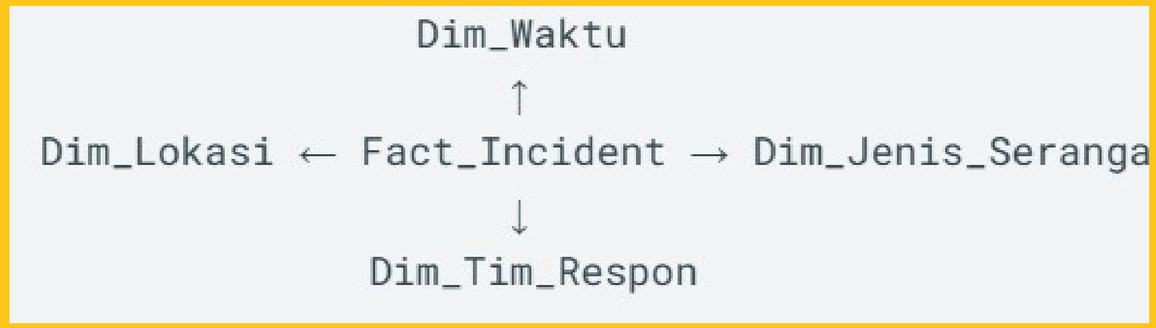
Tabel Dimensi :

- Dim_Waktu
- Dim_Lokasi
- Dim_Jenis_Serangan
- Dim_Tim_Respon

Tabel Fakta :

- Fact_Incident

Skema



Implementation

ETL Process

- Menggunakan staging tables untuk pembersihan data
- Load dimensi terlebih dahulu, kemudian fact
- Proses load menghindari duplikasi dengan kondisi WHERE NOT EXISTS
- Transformasi data sederhana, contohnya standarisasi status penanganan menjadi huruf kapital
- Menggunakan prosedur stored procedure dengan error handling TRY-CATCH dan transaksi

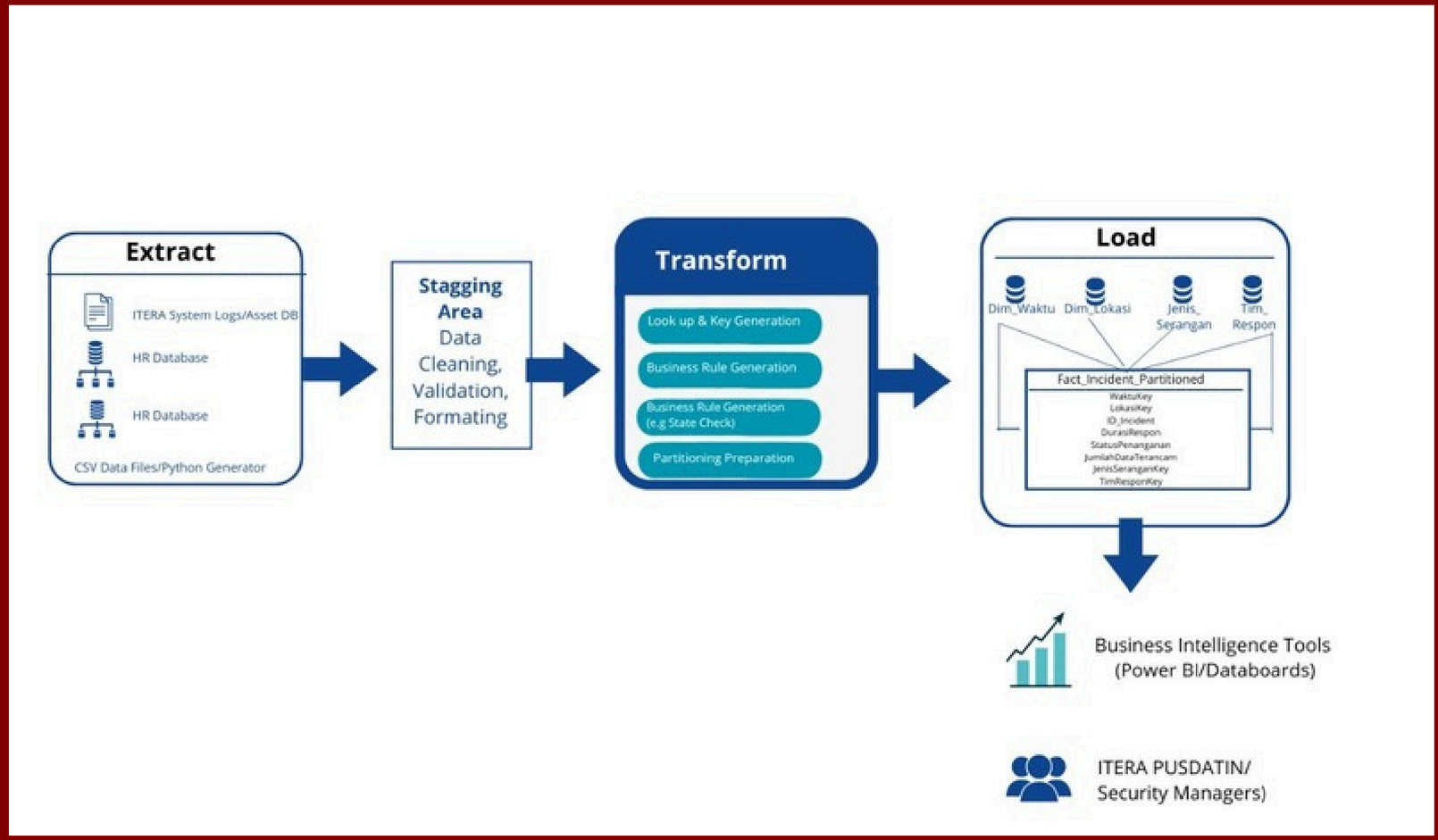
Data Volume & Quaity

- Data insiden sampai sekitar 10.000 kejadian dalam 3 tahun
- Quality checks termasuk pengecekan NULL, referential integrity, validasi status, dan duplikasi ID insiden
- Monitoring jumlah data antara staging dan data warehouse

Challenges & Solutions

- Menjaga konsistensi data antar staging dan final
- Mengelola data histori dengan Slowly Changing Dimensions Tipe 2
- Optimasi query dengan clustered, non-clustered, dan columnstore indexes
- Penanganan partisi data berdasarkan periode (YYYYMMDD) untuk performa

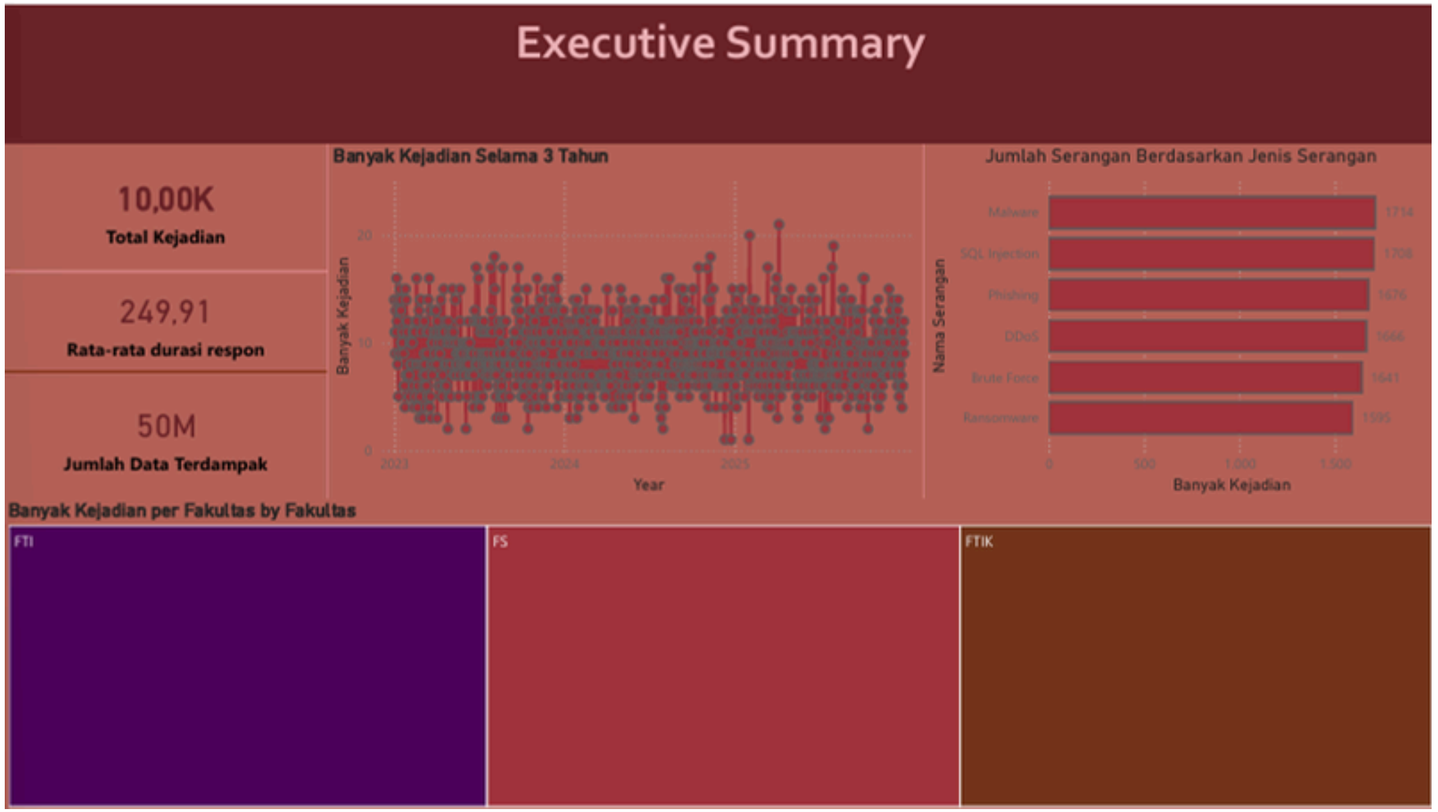
ETL ARCITECTURE DESIGN



ETL MAPPING

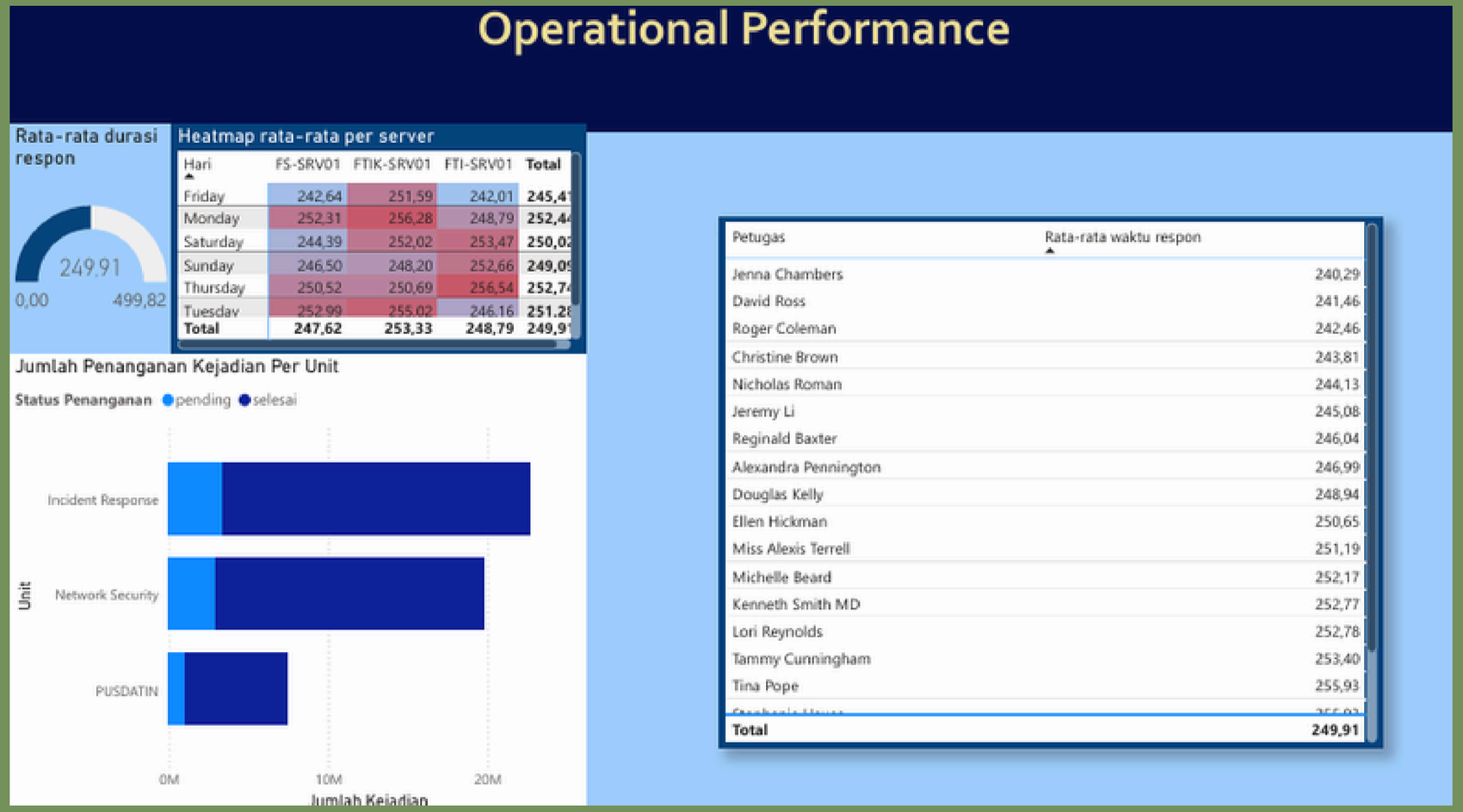
Source	Source Column	Target	Target Column	Transformation
dbo.Dim_Waktu	WaktuKey	Dim_Waktu	WaktuKey	Direct mapping
dbo.Dim_Waktu	Tanggal	Dim_Waktu	Tanggal	Direct mapping
dbo.Dim_Waktu	Bulan	Dim_Waktu	Bulan	Direct mapping
dbo.Dim_Waktu	Tahun	Dim_Waktu	Tahun	Direct mapping
dbo.Dim_Waktu	Hari	Dim_Waktu	Hari	Direct mapping
dbo.Dim_Lokasi	LokasiKey	Dim_Lokasi	LokasiKey	Direct mapping
dbo.Dim_Lokasi	Fakultas	Dim_Lokasi	Fakultas	Direct mapping
dbo.Dim_Lokasi	Server	Dim_Lokasi	Server	Direct mapping
dbo.Dim_JenisSerangan	JenisSeranganKey	Dim_JenisSerangan	JenisSeranganKey	Direct mapping
dbo.Dim_JenisSerangan	NamaSerangan	Dim_JenisSerangan	NamaSerangan	Direct mapping
dbo.Dim_JenisSerangan	Deskripsi	Dim_JenisSerangan	Deskripsi	Direct mapping
dbo.Dim_TimRespon	TimResponKey	Dim_TimRespon	TimResponKey	Direct mapping
dbo.Dim_TimRespon	Petugas	Dim_TimRespon	Petugas	Direct mapping
dbo.Dim_TimRespon	Jabatan	Dim_TimRespon	Jabatan	Direct mapping
dbo.Dim_TimRespon	Unit	Dim_TimRespon	Unit	Direct mapping
dbo.Fact_Incident	ID_Incident	Fact_Incident	ID_Incident	Direct mapping
dbo.Fact_Incident	WaktuKey	Fact_Incident	WaktuKey	Direct mapping (FK sudah tersedia)
dbo.Fact_Incide	LokasiKey	Fact_Incident	LokasiKey	Direct mapping (FK

Dashboard Overview



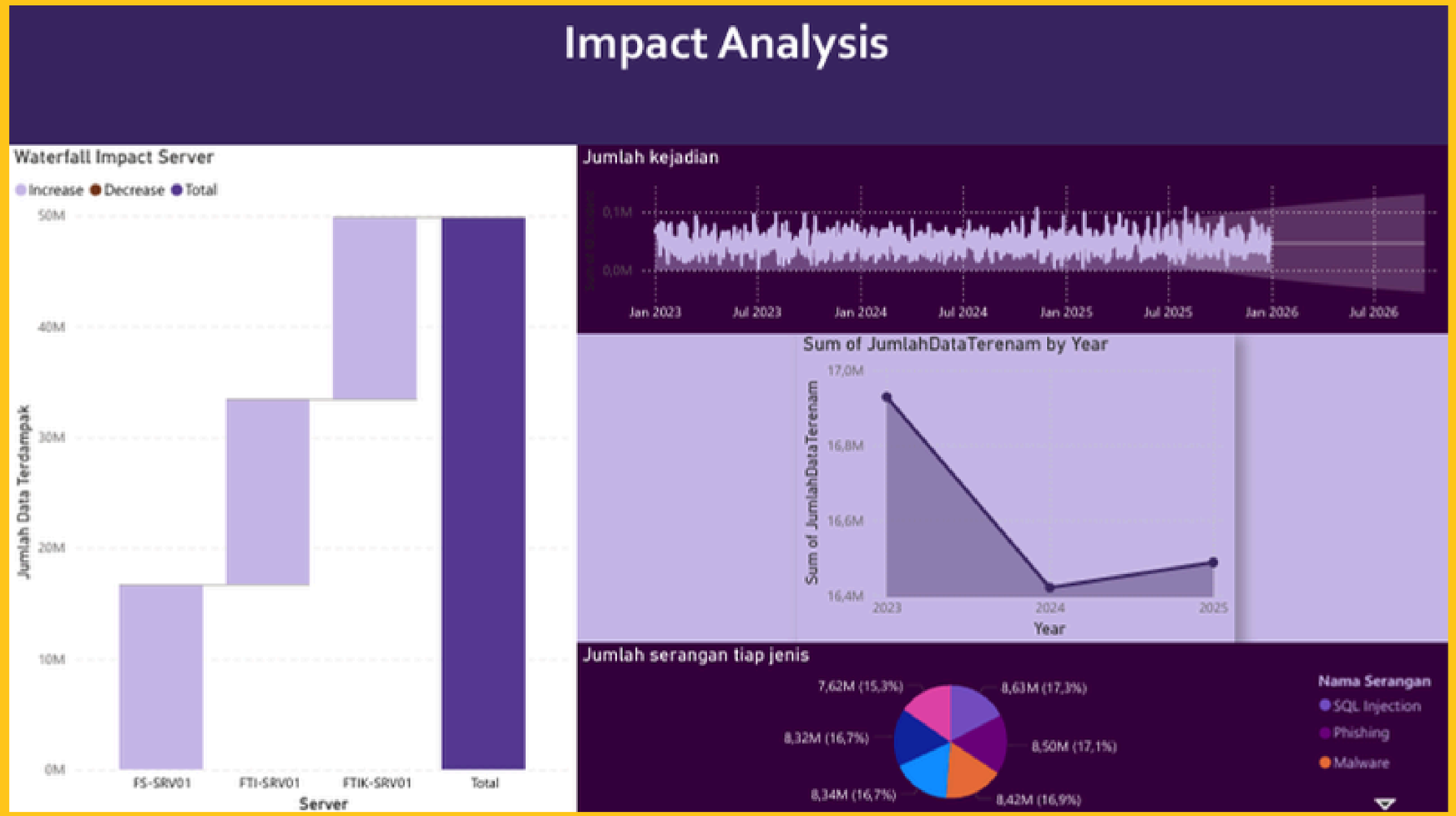
Dashboard Executive Summary: menampilkan tren jumlah insiden, durasi respon, total dampak data

Dashboard Overview



Operational Performance Dashboard: performa petugas, heatmap respon per server dan hari, status penyelesaian

Dashboard Overview



Impact Analysis Dashboard: dampak data per tahun, distribusi dampak per jenis serangan, timeline insiden

Key Features & Interactivity

- Filter waktu (harian, mingguan, bulanan)
- Filter lokasi (fakultas, server)
- Filter jenis serangan
- Drill-down untuk detail insiden dan tim respon

User Scenarios

- Manajer keamanan memantau tren dan prioritas mitigasi
- Koordinator tim evaluasi kinerja petugas
- Staff IT analisis pola serangan teknis

Performance Metrics

- Rata-rata durasi respon insiden sekitar 249 menit
- Total insiden sekitar 10.000 kejadian selama 3 tahun
- Dampak data mencapai 50 juta data terdampak

Optimmization Techniques

Cllustered Index

CIX_Fact_Incident_WaktuKey :

- Dibentuk pada atribut WaktuKey dan IncidentKey.
- Indeks ini mengatur data secara fisik dalam disk berdasarkan urutan waktu.

Non Cllustered Index

A. IX_Fact_Incident_Lokasi
- Dibentuk pada LokasiKey
- Mengikutsertakan atribut DurasiRespon dan JumlahDataTerenam
- Tujuan: Mempercepat analisis per lokasi (fakultas/server).

B. IX_Fact_Incident_JenisSerangan
- Dibentuk pada JenisSeranganKey
- Mengikutsertakan DurasiRespon dan JumlahDataTerenam
- Tujuan: Mempercepat analisis per jenis serangan.

C. IX_Fact_Incident_TimRespon
- Dibentuk pada TimResponKey
- Mengikutsertakan DurasiRespon dan StatusPenanganan
- Tujuan: Mendukung analisis kinerja tim respon.

D. IX_Fact_Incident_Cover
- Indeks gabungan (covering index) pada WaktuKey dan LokasiKey
- Mengikutsertakan: JenisSeranganKey, DurasiRespon, JumlahDataTerenam, StatusPenanganan
- Tujuan: Mempercepat query multidimensi yang menggabungkan tabel dimensi utama

Columnstore Index

Atribut yang digunakan:

- WaktuKey, LokasiKey, JenisSeranganKey, TimResponKey
- DurasiRespon, JumlahDataTerenam, StatusPenanganan

Partitioninng Strategy

Partisi	**Periode Data**
Partisi 1	Data < 1 Januari 2023
Partisi 2	2023
Partisi 3	2024
Partisi 4	2025 dan seterusnya

Security & Backup

Roles yang digunakan:

- db_etl_operator
- db_executive
- db_analyst
- db_viewer

User Roles

Melakukan pencadangan penuh (full backup) database dengan tujuan menjaga keamanan data, memastikan ketersediaan cadangan apabila terjadi kerusakan, dan mempermudah proses pemulihan sistem.

Parameter :

- COMPRESSION
- INIT
- NAME = 'Full Database Backup'
- STATS = 10

Backup & Recovery Strategy

A. ETL Operator

Hak akses yang diberikan:

- EXECUTE: Menjalankan stored procedure ETL utama usp_Master_ETL_KeamananSiber
- SELECT, INSERT, UPDATE, DELETE pada skema stg untuk extract, cleaning, dan prepare data
- INSERT pada skema dbo : Untuk memindahkan data bersih dari staging ke tabel fakta & dimensi

B. Executive

Hak akses yang diberikan:

- SELECT pada seluruh tabel skema dbo untuk membaca data manajemen & laporan strategis
- EXECUTE pada stored procedure ETL untuk monitoring atau menjalankan ulang ETL dalam keadaan darurat

C. Analyst

Hak akses yang diberikan :

- SELECT di skema dbo (data final untuk analisis)
- FULL ACCESS (SELECT, INSERT, UPDATE, DELETE) di skema stg untuk transformasi data, cleaning tambahan, dan preprocessing

D. Viewer

Hak Akses yang diberikan :

- SELECT pada:

1) Fact_Incident
2) Dim_Waktu
3) Dim_Lokasi

Users and Assign Roles

Lessons Learned & Future Work

Key Takeaways

- Pentingnya desain dimensional untuk kemudahan analisis
- Proses ETL yang sistematis mengurangi kesalahan data
- Optimasi indeks dan partisi sangat meningkatkan performa

Challenges Overcome

- Menjaga konsistensi data saat load dan transformasi
- Memastikan data historis tetap terjaga dengan SCD Type 2
- Mengatasi fragmentasi dan blocking query

Potential Improvements

- Implementasi automasi monitoring ETL dan quality checks lebih lanjut
- Integrasi data dari sumber baru untuk cakupan keamanan lebih luas
- Pengembangan dashboard interaktif lebih lanjut

Scalability Considerations

- Skema partisi dan indexing mendukung pertumbuhan data besar
- Perencanaan kapasitas storage dan resource untuk beban kerja yang meningkat