

Kelompok 9 : Keamanan Siber

Anggota :

1. Fadil Prasetyo Alfarizzi (123450048)
2. Reynaldi Rahmad (122450088)
3. Melinza Nabila (123450122)
4. Fathya Intami Gusda (123450095)

Studi Kasus: Keamanan Siber Institut Teknologi Sumatera (ITERA)

3.5.1 Step 1: Business Requirements Analysis

Tujuan: Memahami kebutuhan bisnis dan analitik dari unit kerja keamanan siber untuk pengelolaan insiden keamanan (cyber incident) pada sistem jaringan organisasi.

Aktivitas:

1. Identifikasi Stakeholders

Pengguna utama data mart:

- **Manajer Keamanan Informasi (CISO):** memantau performa keamanan sistem dan tren serangan.
- **Koordinator Tim Respon Insiden:** mengevaluasi waktu respon dan efektivitas tim.
- **Staff Keamanan IT:** melakukan analisis teknis terhadap pola serangan dan titik rawan.
- **Pimpinan Fakultas / Unit TI:** memantau kondisi server dan prioritas mitigasi di masing-masing unit.

Decision Makers:

- Kepala Pusat Data & Keamanan TI.
- Rektor atau Wakil Rektor bidang TI (sebagai pengambil keputusan strategis).

2. Analisis Proses Bisnis

Proses bisnis utama yang terjadi dalam penanganan insiden keamanan meliputi:

1. Deteksi Insiden oleh sistem monitoring.
2. Klasifikasi Jenis Serangan (DDoS, Malware, SQL Injection, dll).
3. Pencatatan Lokasi & Server terdampak.
4. Respon oleh Tim Penanganan (Incident Response Team).
5. Pelaporan hasil dan waktu penyelesaian.

Key Performance Indicators (KPI):

- Rata-rata durasi respon insiden.
- Jumlah insiden per bulan.
- Frekuensi serangan per fakultas/unit.
- Jumlah data yang terdampak.
- Persentase insiden yang diselesaikan tepat waktu.

Metrik Bisnis:

- Durasi respon (menit).
- Jumlah data terdampak (file/data).
- Status penyelesaian (selesai/pending).
- Frekuensi serangan (count per periode).

3. Kebutuhan Analitik

Pertanyaan Bisnis yang perlu dijawab:

- Berapa banyak insiden keamanan yang terjadi setiap bulan?
- Fakultas atau unit mana yang paling sering terkena serangan?
- Jenis serangan apa yang paling sering terjadi?
- Berapa lama rata-rata waktu yang dibutuhkan untuk menangani setiap insiden?
- Siapa anggota tim yang paling cepat merespon serangan?

Jenis Laporan yang Dibutuhkan:

- **Laporan harian:** daftar insiden yang baru terjadi dan status penyelesaiannya.
- **Laporan mingguan:** tren jenis serangan dan aktivitas tim respon.
- **Laporan bulanan:** evaluasi performa tim, jumlah serangan per lokasi, dan durasi respon rata-rata.

Level Agregasi:

- Harian → Mingguan → Bulanan
- Unit → Fakultas → Institusi
- Jenis Serangan → Kategori Serangan

3.5.2 Step 2: Conceptual Design

Tujuan:

Membuat model konseptual yang merepresentasikan entitas bisnis dan hubungan antar entitas pada sistem penanganan insiden keamanan.

Aktivitas:

1. Identifikasi Entitas

Entitas utama:

- **Incident** – kejadian serangan siber yang terdeteksi.
- **Waktu** – dimensi waktu terjadinya insiden.
- **Lokasi** – unit/fakultas/server tempat insiden terjadi.
- **Jenis_Serangan** – tipe serangan yang dialami sistem.
- **Tim_Respon** – tim yang menangani dan menutup insiden.

Atribut utama setiap entitas:

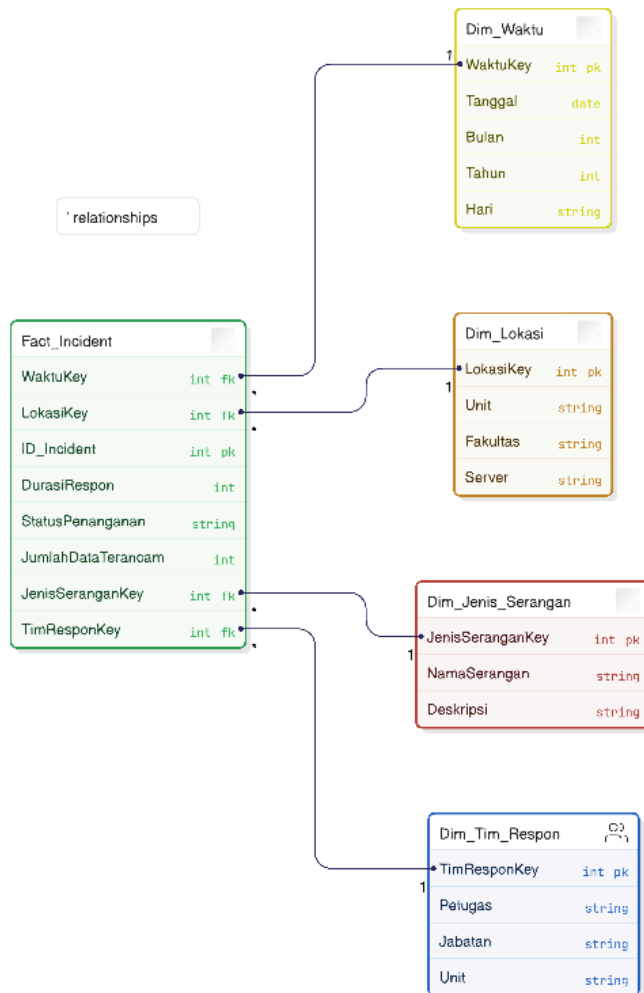
Entitas	Atribut	Primary/Foreign Key
Incident	ID_Incident, WaktuKey, LokasiKey, JenisSeranganKey, TimResponKey, DurasiRespon, StatusPenanganan, JumlahDataTerenam	PK: ID_Incident
Waktu	WaktuKey, Tanggal, Bulan, Tahun, Hari	PK: WaktuKey
Lokasi	LokasiKey, Unit, Fakultas, Server	PK: LokasiKey
Jenis_Serangan	JenisSeranganKey, NamaSerangan, Deskripsi	PK: JenisSeranganKey
Tim_Respon	TimResponKey, Petugas, Jabatan, Unit	PK: TimResponKey

2. Definisi Relationships

Relasi	Kardinalitas	Jenis
Waktu ↔ Incident	1 – N	One-to-Many
Lokasi ↔ Incident	1 – N	One-to-Many
Jenis_Serangan ↔ Incident	1 – N	One-to-Many
Tim_Respon ↔ Incident	1 – N	One-to-Many

Semua hubungan bersifat **mandatory**, karena setiap insiden harus memiliki waktu, lokasi, jenis serangan, dan tim respon yang menanganinya.

3. Gambar ERD



3.5.3 Step 3: Logical Design – Dimensional Model

Tujuan:

Mengonversi model konseptual menjadi model dimensional untuk keperluan analisis pada data warehouse.

Aktivitas:

1. Identifikasi Fact Table

Fact Table: Fact_Incident

- **Business Process:** Pelaporan dan penanganan insiden keamanan.
- **Grain:** Satu record = satu kejadian insiden.
- **Measures:** DurasiRespon, JumlahDataTerenam.
- **Additivity:** Additive.

2. Identifikasi Dimension Tables

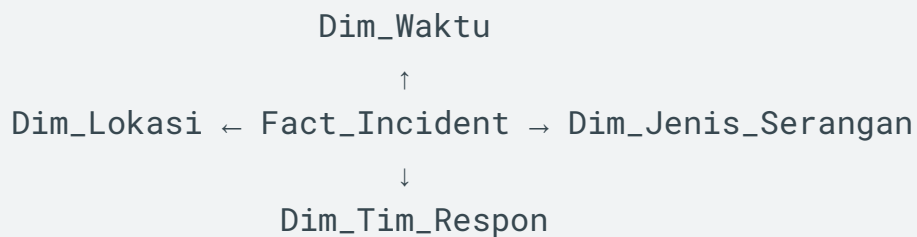
Dimensi	Fokus Analisis	Contoh Atribut
Dim_Waktu	Kapan insiden terjadi	Tanggal, Bulan, Tahun, Hari
Dim_Lokasi	Di mana insiden terjadi	Unit, Fakultas, Server
Dim_Jenis_Serangan	Apa jenis serangan	NamaSerangan, Deskripsi
Dim_Tim_Respon	Siapa yang menangani	Petugas, Jabatan, Unit

3. Desain Star Schema

Fact table berada di tengah, dikelilingi oleh empat dimensi.

Diagram:

Python



Foreign Key Relationships:

- Fact_Incident.WaktuKey → Dim_Waktu.WaktuKey
- Fact_Incident.LokasiKey → Dim_Lokasi.LokasiKey
- Fact_Incident.JenisSeranganKey → Dim_Jenis_Serangan.JenisSeranganKey
- Fact_Incident.TimResponKey → Dim_Tim_Respon.TimResponKey

4. Penentuan Surrogate Keys

- Semua dimensi menggunakan **integer surrogate key**.
- **Naming Convention:**

Dim_Waktu_SK, Dim_Lokasi_SK, Dim_Jenis_Serangan_SK, Dim_Tim_Respon_SK

- Strategi **Slowly Changing Dimensions (SCD)**:

Tipe 2 (History Tracking): bila data tim respon atau lokasi berubah, versi baru dibuat dengan SK baru agar histori tetap terjaga.

3.5.4 Data Dictionary

Tabel	Kolom	Tipe Data	Deskripsi
Fact_Incident	ID_Incident	int (PK)	Kunci utama insiden
	WaktuKey	int (FK)	Referensi ke Dim_Waktu
	LokasiKey	int (FK)	Referensi ke Dim_Lokasi
	JenisSeranganKey	int (FK)	Referensi ke Dim_Jenis_Serangan
	TimResponKey	int (FK)	Referensi ke Dim_Tim_Respon
	DurasiRespon	int	Lama penanganan insiden
	JumlahDataTerenam	int	Banyaknya data terdampak

	StatusPenanganan	string	Status: selesai/pending
Dim_Waktu	WaktuKey	int (PK)	Surrogate key waktu
	Tanggal	date	Tanggal kejadian
	Bulan	int	Bulan ke-n
	Tahun	int	Tahun kejadian
	Hari	string	Nama hari
Dim_Lokasi	LokasiKey	int (PK)	Surrogate key lokasi
	Unit	string	Nama unit kerja
	Fakultas	string	Fakultas terkait
	Server	string	Nama server terdampak
Dim_Jenis_Serangan	JenisSeranganKey	int (PK)	Surrogate key jenis serangan
	NamaSerangan	string	Nama jenis serangan
	Deskripsi	string	Penjelasan singkat
Dim_Tim_Respon	TimResponKey	int (PK)	Surrogate key tim respon
	Petugas	string	Nama petugas
	Jabatan	string	Jabatan petugas
	Unit	string	Unit kerja tim

Repositori:

https://github.com/sains-data/Kelompok9_KeamananSiber.git

The screenshot displays the GitHub web interface for the 'Kelompok9' team. The browser's address bar shows the URL `https://github.com/orgs/sains-data/teams/kelompok9/repositories`. The page header includes the GitHub logo, the organization name 'sains-data', and the team name 'Kelompok9'. A search bar with the placeholder 'Type / to search' is present. Below the header, a navigation bar shows 'Members 1', 'Teams', 'Repositories 1' (which is highlighted), 'Projects', and 'Settings'. The main content area is titled 'Repositories with direct access' and features a search input 'Find a repository...' and a green 'Add repository' button. A table lists the repositories, with one entry visible: 'sains-data/Kelompok9_KeamananSiber', marked as 'Private' and with a role of 'Admin'. The footer of the page contains the GitHub logo, copyright information '© 2025 GitHub, Inc.', and various links like 'Terms', 'Privacy', 'Security', 'Status', 'Community', 'Docs', 'Contact', 'Manage cookies', and 'Do not share my personal information'. The Windows taskbar at the bottom shows the time as 21:31 on 16/11/2025.

Repositories with direct access

Find a repository...

Add repository

Select all

sains-

☐ data/Kelompok9_KeamananSiber

Private

Updated 9 minutes ago

Role: Admin

© 2025 GitHub, Inc. Terms Privacy Security Status Community Docs Contact Manage cookies Do not share my personal information

21:31 16/11/2025