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