Agentic GTM System Architecture

Submitted by: Leon Basin

Context: Founding Engineer Exercise
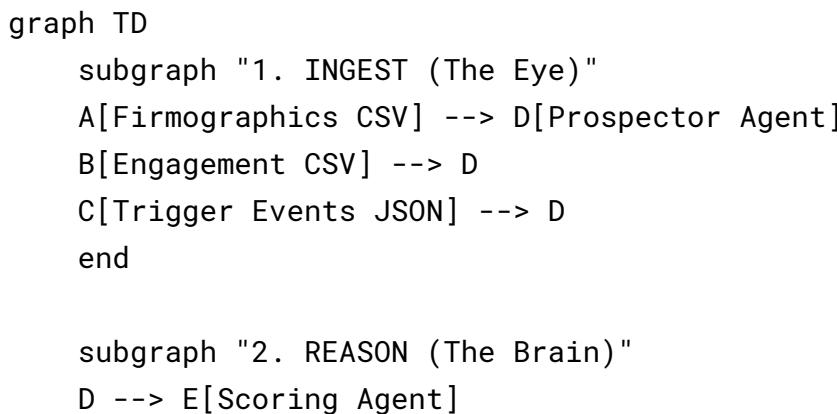
---

1. Executive Summary

This system reimagines the BDR function as an **Event-Driven Agent Swarm**.

It was architected to mirror the core philosophy of **Ambient Pulsar**: moving from reactive "Motion Detection" (Raw Web Visits) to proactive "Threat Assessment" (Contextual Buying Signals).

> **The Shift:** Standard BDR tools filter for *Activity*. This system filters for *Intent*.

---

2. System Architecture

The workflow consists of three distinct stages: **Ingest (The Eye)**, **Reason (The Brain)**, and **Action (The Output)**.

```
graph TD
    subgraph "1. INGEST (The Eye)"
    A[Firmographics CSV] --> D[Prospector Agent]
    B[Engagement CSV] --> D
    C[Trigger Events JSON] --> D
    end

    subgraph "2. REASON (The Brain)"
    D --> E[Scoring Agent]
```

```
E -->|Normalize Data| F{Context Logic}
F -->|Trigger: Breach/Hire| H[Score Multiplier (+50)]
F -->|Trigger: Competitor| G[Kill Switch (Score = 0)]
end

subgraph "3. ACTION (The Output)"
H --> J[Personalization Agent]
J --> K[Prioritized Sales Sequence]
G --> L[Strategy/Intel Route]
end
```

3. Agent Logic Breakdown

The Scoring Agent (Context > Motion)

Standard lead scoring is linear (Clicks + Visits). This system uses **Contextual Multipliers** to prioritize urgency over mere activity.

- **Verified Threat (+50 points):** Events like "Data Breach" indicate immediate pain.
- **Strategic Window (+30 points):** Events like "New CISO" indicate a re-evaluation of the security stack.
- **Standard Motion (Baseline):** Web visits and clicks provide the base score.

The "Friend or Foe" Protocol (Competitor Detection)

The system includes a defensive layer to protect IP and save time.

- **Logic:** If `Trigger Event` contains "Launched Competitive Product" (e.g., Hooli):
- **Action:** Score is forced to `0`.
- **Routing:** The account is removed from the Sales Queue and routed to the Strategy Team for competitive analysis.

The Personalization Agent

Instead of generic templates, the agent constructs messaging based on the *Trigger Event*.

- **Input:** "Initech" + "Data Breach"
- **Output Hook:** "Saw the breach news. Legacy systems detect 'motion' but miss 'intent'. Ambient Pulsar prevents this."

---

4. Future Roadmap & Extensibility

As a Founding Engineer, I view this Python script as the MVP (Phase 1). Here is the roadmap for scaling this into a production engine:

Phase 2: Intelligence (LLM Integration)

- **Objective:** Replace hard-coded hooks with dynamic generation.
- **Implementation:** Connect `Scoring Agent` to OpenAI API. Pass the *Ambient.ai Whitepaper* as context to generate hyper-personalized emails referencing the prospect's specific security stack.

Phase 3: Real-Time (Event Streams)

- **Objective:** Move from Batch (CSV) to Real-Time.
- **Implementation:** Replace CSV ingestion with Webhook listeners (e.g., listening for LinkedIn Job Change API or Clearbit Reveal API). Signals are processed in milliseconds.

Phase 4: Feedback Loop (Reinforcement Learning)

- **Objective:** Auto-tune scoring weights.

- **Implementation:** Ingest "Reply Rates" and "Meeting Booked" data from Salesforce. If "New CISO" leads convert at 20%, automatically increase the score weight from +30 to +40.

Built for Ambient.ai Interview • January 2026