**End-to-End Architecture**

graph TD

%% Sources

SNOW[ServiceNow Incidents\n(short\_desc, category, caller, cmdb\_ci, opened\_at...)]

ATER[Aternity/Alteryx Events\n(device\_name, event\_name, component, severity, event\_time...)]

%% Staging & Normalization

SNOW --> S1[stg\_incident\nUTC times • normalized user/email • cleaned text]

ATER --> S2[stg\_event\nUTC times • normalized hostname • typed severity]

%% Ontology Mapping

S1 --> IO1[IO Mapper\nRules (regex) → IO labels]

S2 --> IO2[IO Mapper\nRules (regex) → IO labels]

IO1 --> UIO[Unified Incident Ontology (IO)\n(domain • component • symptom • cause\_signal)]

IO2 --> UIO

%% Semantic Backstop

UEMB[Embeddings Backstop\nkNN to IO label library] --> UIO

S1 -. text if rules miss .-> UEMB

S2 -. text if rules miss .-> UEMB

%% Linker

UIO --> RL[Record Linker\nWeighted: device • user • time • IO]

S1 --> RL

S2 --> RL

%% Bridge and Products

RL --> BRIDGE[(bridge\_incident\_event)\nincident\_id • event\_id • score]

BRIDGE --> BI[Analytics Views/Dashboards\nvw\_correlated\_issues • MTTR • deflection • swap list]

BRIDGE --> FLOW[SNOW Automations\nAuto-attach evidence • Proactive tickets • Routing]

%% Feedback & CMDB hygiene

HIL[Human-in-the-Loop Labeler\nfix IO & links] --> UIO

AINV[Aternity Inventory → CMDB sync\nhostname • serial • primary user] --> SNOW

**Data Model (compact ER)**

erDiagram

STG\_INCIDENT ||--o{ BRIDGE\_INCIDENT\_EVENT : links

STG\_EVENT ||--o{ BRIDGE\_INCIDENT\_EVENT : links

IO\_LABELS ||--o{ STG\_INCIDENT : assigns

IO\_LABELS ||--o{ STG\_EVENT : assigns

STG\_INCIDENT {

string incident\_id PK

timestamp opened\_at

string caller\_email

string cmdb\_ci

string short\_description

string io\_key FK

}

STG\_EVENT {

string event\_id PK

timestamp event\_time

string device\_name

string user\_email

string health\_event\_name

string severity

string io\_key FK

}

IO\_LABELS {

string io\_key PK

string domain

string component

string symptom

string cause\_signal

}

BRIDGE\_INCIDENT\_EVENT {

string incident\_id FK

string event\_id FK

float score

timestamp linked\_at

}

**Example Flow (sequence)**

sequenceDiagram

participant A as Aternity

participant L as Record Linker

participant N as ServiceNow

participant H as Hardware Team

participant B as BI/Dashboard

A->>L: Event @10:15\nDELL5420H4FQ0J3\n"HD Bad Blocks" (Critical)

N->>L: Incident @12:40\n"System very slow", category=Hardware Failure

L->>L: Map both → IO = End-User Device|Disk|Degradation|HD bad blocks

L->>L: Score = 0.45(device) + 0.25(user) + 0.20(time) + 0.10(IO) ≈ 0.85

L-->>N: Link created (bridge table)\nAttach evidence + KB

N-->>H: Proactive ticket: "Replace disk / swap device"

L-->>B: Surface in vw\_correlated\_issues → “Devices to swap this week”

**Minimal Rules + Scoring**

**Seed IO rules**

* Aternity: (?i)hd bad block → End-User Device|Disk|Degradation|HD bad blocks
* Aternity: (?i)(application|background) process crash → Application|OS Process|Crash|process crash
* SNOW: (?i)\b(wifi|network|vpn|disconnect)\b → Network|NIC/VPN|Disconnected
* SNOW: (?i)\b(battery|ups)\b & category=Hardware → End-User Device|Battery/UPS|Low Battery

**Linker (weights you can tune)**

* 0.45 \* device\_match (exact=1, normalized=0.7, near=0.4)
* 0.25 \* user\_match (email/UPN aliases table)
* 0.20 \* time\_decay (e.g., exp(-|Δt|/6h) up to 48h)
* 0.10 \* io\_match (domain+component exact=1; domain-only=0.5)

Thresholds: ≥0.75 = linked, 0.55–0.75 = review.

**What this delivers (tight and measurable)**

* A single **vw\_correlated\_issues** powering: proactive device swaps, resolver copilot (auto-evidence + KB), and clean routing by component.
* KPIs: correlation coverage, MTTR reduction, proactive completion rate, and deflection for recurring endpoint issues.

**FLOW DIAGRAM**

**A diagram of a data flow

AI-generated content may be incorrect.**

**Case Studies (from your screenshots)**

CS-1: “Laptop slow” → Disk HD Bad Blocks (Critical)

* Aternity: DELL5420H4FQ0J3, event “HD Bad Blocks,” severity Critical.
* SNOW: “System is very slow,” category Hardware Failure.
* IO: End-User Device|Disk|Degradation|HD bad blocks.
* Result: Linked score ~0.85. Auto-open proactive replace; MTTR drops; data-loss risk reduced.

CS-2: “User cannot be heard on Avaya”

* Aternity: Process crash SenseTvm.exe or FwSwitchService.exe near call time; IO → Application|OS Process|Crash.
* SNOW: “Cannot be heard while using Avaya One-X,” category Connectivity/Audio.
* IO alignment: Application|Avaya/Voice|No Sound (text embedding maps “cannot be heard” to “No Sound”).
* Result: Auto-attach crash evidence + headset diagnostics KB; right routing to Voice support.

CS-3: “Server availability threshold violation”

* Aternity/Monitoring: AppDynamics “server availability threshold” alert.
* SNOW: Monitoring Alert ticket.
* IO: Server/Infra|Availability|Threshold Violation|AppDynamics.
* Result: Clear infra ownership; combine with device impact counts for business severity.

**KPIs to Track**

* **Correlation coverage:** % incidents with linked health signal (target 20–35%).
* **MTTR reduction:** linked vs non-linked (target 25–40% faster).
* **Proactive actions:** count of auto-opened replacements; % completed within 5 business days.
* **Deflection rate:** repeating endpoint issues resolved via KB without L2 handoff.

**Unified Incident Ontology (IO)**

Four levels keep it simple and expressive.

* **domain:** End-User Device | Server/Infra | Network | Application | Peripheral
* **component:** Disk | Audio | Battery/UPS | CPU | Memory | NIC/Wi-Fi | VPN | OS Process | AppX | Printer | Avaya/Voice …
* **symptom:** Crash | Not Working | Degradation | Disconnected | No Sound | Login Fail | Threshold Violation | Bad Blocks | Low Battery …
* **cause\_signal:** optional detail (e.g., HD bad blocks, SenseTvm.exe crash, AppDynamics threshold)

**Seed rule examples**

* Aternity health\_event\_name ~ 'HD Bad Blocks' → End-User Device|Disk|Degradation|HD bad blocks
* Aternity '(Application|Background) Process Crash' → Application|OS Process|Crash|process crash
* SNOW text (?i)\b(wifi|vpn|network|disconnect)\b → Network|NIC/VPN|Disconnected
* SNOW category Hardware Failure & text (?i)\b(battery|ups)\b → End-User Device|Battery/UPS|Low Battery

**Semantic backstop:** embed free text (SNOW message; Aternity name/component) and nearest-neighbor to a small labeled IO phrase library when rules miss (cosine ≥ 0.65).

**Record Linker (manufactured join key)**

Score each incident–event pair within a time window.

**Features (weights you can tune)**

* Device match (hostname/CI) → **0.45**
* User match (email/username) → **0.25**
* Time proximity (Δt ≤ 24–48h, exponential decay) → **0.20**
* IO match (same domain+component) → **0.10**

**Decision**

* score ≥ **0.75** → **linked**
* 0.55–0.75 → **review**
* <0.55 → unlinked

Persist to bridge\_incident\_event(incident\_id, event\_id, score).