Detailed Blueprint — Umbrella Intelligence Dashboard

Purpose. Deliver a multi-tenant, executive-grade security intelligence dashboard powered exclusively by Cisco Umbrella. The product fuses posture at a glance with deep, analyst-level drill-downs and an AI narrative that tells leaders what changed, why it matters, and what to do next.

Index

1) Executive Summary & Posture — Developer Spec

1.0 Purpose & UX contract

Deliver a 60-second “airport-walk” briefing: (a) what changed vs last week, (b) why it matters for the business, and (c) the top actions to take—supported by KPI cards with WoW deltas and 8-week sparklines. Narrative bullets must deep-link to the exact evidence view with filters frozen.

1.1 Content model (widgets on the page)

A) Narrative tiles (top row)

- **What changed?** Three bullets with WoW deltas (e.g., “+35% phishing attempts targeting Finance”).
- **So what?** Business translation of risk.
- **Now what?** Three prioritized actions with **Owner** and **ETA**; each bullet links to evidence.
  Deep links open the relevant Threat/Identity/Shadow-IT views with the same tenant/week filters.

B) KPI cards (RAG + WoW + sparkline + tooltip)

Each card shows: **value**, **RAG status** (tenant-tunable thresholds), **ΔWoW**, and an **8-week sparkline**; tooltip explains formula, window, and data source. Cards (minimum set):

- **Global Risk Index (0–100).**
  Formula (default weights): GRI = 0.5·Norm(Threat Severity) + 0.3·Norm(Identity Risk) + 0.2·Norm(Shadow IT Exposure) (lower is better).
- **Total Threats Blocked (weekly sum).**
- **High-Risk Destinations Encountered (unique malicious domains/IPs ≥ severity/risk threshold).**
- **Agent Coverage % (licensed users with active, recently-synced roaming client).**
- **TLS Inspection % (inspected SWG traffic / total SWG traffic).**
- **High-Risk Shadow IT Sessions.**
- **Incident Response SLA % (P1 MTTD/MTTR targets met—optional ticketing integration).**
- **License Utilization %.**

Default RAG (edit per tenant): Coverage <85% Red, 85–95% Amber, ≥95% Green; TLS <60% Red, 60–80% Amber, ≥80% Green; GRI ≥70 Red, 50–69 Amber, <50 Green.

1.2 Data sources → marts → API endpoints

Source → Core/Marts

- Umbrella **Reports v2** + **Investigate** feed **core** facts and **weekly marts** used here (e.g., mart.weekly_kpis_umbrella, mart.exec_delta_weekly).
- AI narratives land in ai.weekly_exec; insights/recs in ai.insights / ai.recommendations.

Relevant mart tables & keys

- mart.weekly_kpis_umbrella (tenant_id, iso_year, iso_week) → KPI card values (block_rate_pct, tls_inspection_pct, agent_coverage_pct, global_risk_index, …).
- mart.exec_delta_weekly (tenant_id, iso_year, iso_week, kpi_key) → WoW absolute/pct deltas rendered beneath each card.
- ai.weekly_exec (tenant_id, iso_year, iso_week) → **headline** + **bullets** + **kpi_snapshot** + **action_summary** for the narrative tiles.

Backend endpoints used by this section

- GET /v1/umbrella/kpis-weekly?tenant_id&iso_year&iso_week – KPI card payload.
- GET /v1/umbrella/risk-semaphore?tenant_id&iso_year&iso_week – (optional small strip under headline).
- GET /v1/ai/weekly-exec?tenant_id&iso_year&iso_week – narrative tiles (What/So What/Now What).
  Caching: ETag/If-None-Match (TTL 60–300s).

Non-functional budgets for these endpoints: P95 latency < **500 ms** for marts; freshness: events hourly, current-week trend refresh hourly, marts nightly.

1.3 Field-level contracts (response shapes)

A) /v1/umbrella/kpis-weekly

```
{
  "tenant_id": "uuid",
  "iso_year": 2025,
  "iso_week": 33,
  "total_dns": 87400000,
  "security_blocks": 1280000,
  "block_rate_pct": 1.46,
  "malicious_domains_blocked": 34567,
  "tls_inspection_pct": 78.2,
  "agent_coverage_pct": 96.4,
  "global_risk_index": 42.7,
  "license_utilization_pct": 88.5
}
```

Backed by mart.weekly_kpis_umbrella; all percentages constrained [0..100].

B) /v1/umbrella/risk-semaphore

```
{
  "tenant_id":"uuid","iso_year":2025,"iso_week":33,
  "malware_level":"AMBER","phishing_level":"RED","cnc_level":"AMBER",
  "cryptomining_level":"GREEN","rc_outdated_level":"GREEN"
}
```

Backed by mart.risk_semaphore_weekly.

C) /v1/ai/weekly-exec

```
{
  "tenant_id":"uuid","iso_year":2025,"iso_week":33,
  "headline":"Credential phishing rising in Finance; TLS visibility improving.",
  "bullets":[
    {"type":"WHAT_CHANGED","text":"+35% phishing vs last week", "evidence_link":"/threats?tab=phishing&week=2025-W33"},
    {"type":"SO_WHAT","text":"Elevated credential compromise risk in a critical unit", "evidence_link":"/identities?bu=Finance"},
    {"type":"NOW_WHAT","text":"Run targeted awareness; tighten newly-seen domain policy","owner":"SecOps","eta":"2025-08-23","evidence_link":"/policy-sim?rule=newly_seen>=80"}
  ],
  "kpi_snapshot":{"gri":42.7,"tls_inspection_pct":78.2,"agent_coverage_pct":96.4},
  "action_summary":{"open_critical":3,"due_this_week":5}
}
```

Backed by ai.weekly_exec generated by the AI run.

List responses (where applicable) follow { items: [...], meta: { count, page, page_size, next } }.

1.4 KPI computation notes (server-side)

- **GRI**: compute from normalized components (0..100) derived from weekly marts:

    - *Threat Severity* from security_blocks and mix (weight high-severity families).
    - *Identity Risk* from top identities / risk scores aggregated for week.
    - *Shadow-IT Exposure* from shadowit_flags_weekly and high-risk sessions.
      Persist result in mart.weekly_kpis_umbrella.global_risk_index.
- **WoW deltas**: materialize into mart.exec_delta_weekly (kpi_key, wow_abs, wow_pct) and join for card footers.
- **TLS Inspection %**: from SWG marts (inspected/total SWG requests). **Agent Coverage %** from RC health marts (rc_outdated_weekly.coverage_pct complements coverage KPIs).
- **Identity/SLA/License KPIs**: SLA% is optional (ServiceNow/Jira integration). License Utilization % pulled from infra/licensing aggregation surfaced in the same weekly mart.

Time semantics: store timestamps in UTC; present ISO Week (Mon–Sun) in Europe/Madrid; marts keyed by (tenant_id, iso_year, iso_week).

1.5 RAG thresholds & tenant config

- Provide defaults (see §1.1) and allow per-tenant overrides in meta.feature_flags or a small meta.settings table.
- Tooltip on each card shows thresholds currently in effect.

1.6 Bubble wiring (frontend binding)

- Bind **KPI cards** to /v1/umbrella/kpis-weekly; small helper group computes RAG from thresholds returned alongside or from tenant settings.
- Bind **narrative tiles** to /v1/ai/weekly-exec; each bullet's **evidence_link** is used by the on-click action (open evidence view with frozen filters).
- Optional small **risk semaphore** strip uses /v1/umbrella/risk-semaphore.
- Use Bubble API Connector with auth headers; consider cache invalidation webhook after marts complete.

1.7 Caching, errors & graceful degradation

- **Caching**: ETag/If-None-Match (hash of tenant_id + query params + latest_updated_at). TTL 60–300s.
- **Investigate outage**: deliver KPI cards from marts; mark enrich-dependent bullets with a **stale** badge (age of enrichment shown).
- **Partial data** (new tenant / first week): render cards without sparkline; narrative shows a neutral "insufficient history" message.
- **No data** for the week: empty state with CTA to check ingest status (link to Infra/RC Health).

1.8 Performance & scheduling

- **Performance budgets**: P95 < **500 ms** for mart endpoints; P95 < **1.5 s** for heavy Top-N (not used here).
- **Freshness**: events hourly; current-week sparkline re-computed hourly; marts nightly.

1.9 Security & multitenancy

- Every table and endpoint guarded by tenant_id (row-level isolation).
- Secrets in env vars; audit all API calls; throttle per tenant; circuit breaker on Cisco 429/5xx.

1.10 Acceptance tests (traceable)

1. KPI cards show **value + ΔWoW + sparkline** and tooltips with definition & data source; GRI matches server-side materialization.
2. Narrative tiles render **What/So What/Now What**; each bullet's evidence link opens the correct filtered view.

3. RAG status respects tenant thresholds; toggling thresholds flips card colors accordingly.
4. Empty/partial data states render without console errors; stale badges appear if enrichment is older than policy threshold.
5. Endpoint responses conform to contracts and ETags are honored (304 on unchanged).

1.11 Implementation hints (server side)

- Precompute weekly metrics into mart.weekly_kpis_umbrella; compute WoW deltas into mart.exec_delta_weekly; aggregate narrative into ai.weekly_exec.
- Index marts on (tenant_id, iso_year, iso_week); retain marts for 24 months. Facts retain 90 days; use BRIN for time-series.

1.12 Example pseudo-SQL (GRI materialization)

```
-- Example: compute GRI and persist in mart.weekly_kpis_umbrella
WITH s AS (
  SELECT tenant_id, iso_year, iso_week,
         security_blocks, tls_inspection_pct, agent_coverage_pct
  FROM mart.weekly_kpis_umbrella
),
id_risk AS (
  SELECT tenant_id, iso_year, iso_week,
         PERCENTILE_CONT(0.9) WITHIN GROUP (ORDER BY risk_score) AS id_risk_p90
  FROM mart.top_identities_weekly
  GROUP BY 1,2,3
),
shadow AS (
  SELECT tenant_id, iso_year, iso_week,
         COALESCE(high_risk_new,0) AS shadow_flags
  FROM mart.shadowit_flags_weekly
)
UPDATE mart.weekly_kpis_umbrella m
SET global_risk_index =
  0.5 * norm_threat(security_blocks) +
  0.3 * norm_identity(id.id_risk_p90) +
  0.2 * norm_shadow(sh.shadow_flags)
FROM s
JOIN id_risk id USING (tenant_id, iso_year, iso_week)
JOIN shadow sh USING (tenant_id, iso_year, iso_week)
WHERE m.tenant_id=s.tenant_id AND m.iso_year=s.iso_year AND m.iso_week=s.iso_week;
```

(Use server-side norm_* helpers consistent with your AI baselines.)

Appendix: Quick mapping (widget → table → endpoint)

- Narrative tiles → ai.weekly_exec → /v1/ai/weekly-exec (Bubble text/list).
- KPI cards → mart.weekly_kpis_umbrella + mart.exec_delta_weekly → /v1/umbrella/kpis-weekly.
- Risk strip (optional) → mart.risk_semaphore_weekly → /v1/umbrella/risk-semaphore.

2) Threat Landscape & Adversary Intelligence — Developer Spec

Component

A deep-dive area that turns Umbrella telemetry + Investigate enrichment into **time-based trends, adversary context (Geo/ASN/families)**, **top entities** and **early-warning signals**. It powers hunt workflows and informs prioritized remediation.

Primary widgets on page (unchanged design):

- Threat Trends by type (8-week) with 13-week bands
- Advanced Threat Heatmap (Hour × Day × Category)
- Total threats by identity type
- Top 10 destinations / identities with ΔWoW
- DNS query-type analytics
- Adversary Geo & ASN
- Campaign clustering (threat families)
- Early-Warning spotlight
- MITRE ATT&CK mapping panel

Content (with implementation details)

2.1 Threat Trends by Type with Seasonality

What it shows: 8-week threat volumes overlaid with 13-week confidence bands to separate normal seasonality from true anomalies.

Data model (read-optimized marts):

- mart.trend_critical_blocks_4w (tenant_id, week_start, threat_family): weekly series for high-severity families. Extend to 8w in query window.

Endpoint & params:

- GET /v1/umbrella/trend-critical-4w?tenant_id&from=YYYY-Www&to=YYYY-Www&family=phishing,malware,cnc (supports multiple families; returns ≥8 weeks plus calculated bands).

Response contract (example):

```
{
 "items":[
  {"week_start":"2025-06-30","family":"phishing","count":3120,"band_low":2400,"band_high":3600},
  {"week_start":"2025-07-07","family":"phishing","count":3550,"band_low":2450,"band_high":3650}
 ],
 "meta":{"count":8}
}
```

Computation notes: Bands are computed server-side using the prior 13 weeks (P10/P90 or μ±1.28σ), cached with ETag (TTL 60–300s).

UX binding: Bubble line chart with toggle chips for families; anomaly points highlighted when count > band_high.

2.2 Advanced Threat Heatmap (Hour × Day × Category)

What it shows: Attack windows by hour & weekday per security category. Source: Umbrella reports categories by hour.

Data model:

- mart.heatmap_hourly_week (tenant_id, iso_year, iso_week, dow, hour, threat_family, count); refresh hourly for current week.

Endpoint:

- GET /v1/umbrella/heatmap?tenant_id&iso_year&iso_week&family=*

Acceptance tests: Filtering by family updates cells; hovering shows exact counts; switching week preserves tenant scope.

2.3 Total Threats by Identity Type

What it shows: Distribution of blocks by identity kind (user, roaming computer, network, site).

Data model & Top-N:

- mart.top_identities_weekly (tenant_id, iso_year, iso_week, identity_sk, blocks, risk_score, rank) (index tuned for Top-N).

Endpoint:

- GET /v1/umbrella/top-identities?tenant_id&iso_year&iso_week&limit=10&by_type=true (groups by Umbrella identity type).

ΔWoW calculation: For stacked bars, call same endpoint for current and prior week and compute Δ client-side (or use rank snapshots).

2.4 Top 10 Destinations / Identities with ΔWoW

What it shows: Week's risers and fallers with % change.

Data model:

- mart.top_domains_weekly (tenant_id, iso_year, iso_week, domain_sk, threat_family, blocks, rank); pair with prior week to compute ΔWoW.

Endpoints:

- GET /v1/umbrella/top-domains?tenant_id&iso_year&iso_week&limit=10
- GET /v1/umbrella/top-identities?tenant_id&iso_year&iso_week&limit=10

Client behavior: Fetch current & prior week, compute delta_pct = (now - prev)/max(1, prev). Render ▲/▼ chips.

2.5 DNS Query-Type Analytics

What it shows: Spikes in TXT/NULL/AAAA suggesting tunneling/abuse; rank by identity.

Data model:

- Extend marts or store per-week aggregates in mart.advanced_detections_weekly (… detection ∈ {TUNNELING}) with examples.

Acceptance tests: Displays % distribution by identity; clicking an identity opens last-N queries with cross-refs to Investigate risk.

2.6 Adversary Geo & ASN

What it shows: Top countries and ASNs of malicious infra (WoW "new/fast-rising" flag). Data: Investigate IP/ASN/WHOIS + Umbrella volumes.

Data model (relations):

- Store domain→IP→ASN pivots and weekly rollups; optional edges in mart.domain_relation_weekly for infra context.

UX: Map + table; new/fast-rising if now_rank <= 10 && (prev_missing || delta_pct ≥ threshold).

2.7 Campaign Clustering (Threat Families)

What it shows: Domain clusters via Investigate Related/Co-occurrence; one-click **Add family to Destination List**.

Data model:

- Persist edges in mart.domain_relation_weekly (src_domain_sk, dst_domain_sk, edge_weight); attach weekly metrics for each family.

Flow:

- Build graph → community detection (Louvain) → families with domains_count, combined_blocks, max_risk_score, top_ASNs → POST to Destination Lists in chunks.

2.8 “Early-Warning” Spotlight

What it shows: Newly-seen domains with **medium/high risk** that received **allowed hits** this week (policy gap).

Rule (server): is_newly_seen AND risk_score ≥ {tenant_threshold} AND allowed_hits_week > 0 → list candidates with simulate-block, add-to-list, or time-boxed exception actions.

Data model: Use mart.advanced_detections_weekly (NEWLY_SEEN) + join allowed summaries.

2.9 MITRE ATT&CK Mapping

What it shows: Weekly volumes mapped to techniques (e.g., T1566 Phishing, T1071.004 DNS C2), with **control coverage** (which Umbrella policies fired).

Implementation: Static mapping table {threat_family → [techniques...]} + weekly aggregates render ATT&CK-style heat cells; show which policy categories hit (Malware, C2, Newly Seen).

Core Insight / Purpose

Move from **“what happened”** to **“who is attacking, how, when, and what’s next”**, surfacing **campaigns, weak controls, and windows of exposure**—actionable for SecOps and defensible for leadership.

Added for the developer (without altering design)

A) Data contracts & endpoints (public)

Use the following read APIs; all return list envelopes { items, meta }, honor ETag, and target P95 < 500 ms (1.5 s for heavy Top-N).

- /v1/umbrella/trend-critical-4w — trends + bands
- /v1/umbrella/heatmap — hour×day heatmap
- /v1/umbrella/top-identities — Top identities (optionally grouped by type)
- /v1/umbrella/top-domains — Top malicious destinations
- (Optional) /v1/umbrella/weekly-evolution — day-over-day within week (sparklines)

Example for /v1/umbrella/top-domains:

```
{
 "items":[
  {
   "domain":"evil.example",
   "family":"cnc",
   "blocks":1240,
   "delta_wow_pct":85.3,
   "risk_score":92,
   "asn_name":"AS13335",
   "asn_number":13335
  }
 ],
 "meta":{"count":10}
}
```

B) Marts you must populate nightly / hourly

- **Nightly (gold):** mart.trend_critical_blocks_4w, mart.top_domains_weekly, mart.top_identities_weekly, mart.advanced_detections_weekly, mart.domain_relation_weekly.
- **Hourly (current week):** mart.heatmap_hourly_week, plus incremental refresh of evolution/day-splits.

C) Calculations (server-side)

- **ΔWoW:** (this_week - prev_week)/max(1, prev_week). Apply to domains & identities.
- **Ranking composite (Top domains):** 0.5·pct(risk_score) + 0.3·severity(family) + 0.2·z(blocks); tie-break by impacted identities then ΔWoW.
- **Early-warning:** join Investigate risk + WHOIS age + allowed hits this week; return action links.

D) Bubble wiring & UX rules

- Heatmap filter chips (Malware/Phishing/C2) drive the API family param and repaint within 200 ms; tooltip shows count + local time.
- Trend chart toggles families; anomaly dots show “Outside seasonal band”.
- Top lists are **sortable** by blocks or delta_wow_pct; clicking a row opens a right-hand drawer with Investigate facts and related graph preview.

E) Performance, freshness, retention

- **P95 latency:** 500 ms for marts; 1.5 s for Top-N with joins/enrichment.
- **Freshness:** facts hourly; current-week heatmap hourly; marts nightly.
- **Retention:** facts 90 days; marts 24 months (per-tenant configurable).

F) Error & empty states

- **No data this week:** show neutral empty state and a link to ingest health.
- **Investigate 429/5xx:** degrade gracefully—render Umbrella-only data and stamp a “stale Investigate” badge. (ETag + backoff recommended.)

G) Acceptance tests (traceable)

- Heatmap responds to family filter and week switch; values match API.
- Top 10 lists display **ΔWoW** correctly when prior-week = 0 (guard by max(1, prev)).
- Campaign clustering creates families and supports **Add family to Destination List** with chunked POST.
- Early-warning table only lists domains meeting all three conditions (newly-seen, risk threshold, allowed hits).
- MITRE panel shows volumes per technique and indicates which Umbrella policy fired.

Data lineage quick map (for dev handoff)

Widget → Mart(s) → Endpoint

- **Trend 8w** → mart.trend_critical_blocks_4w → /v1/umbrella/trend-critical-4w
- **Heatmap 7×24** → mart.heatmap_hourly_week → /v1/umbrella/heatmap
- **Top identities** → mart.top_identities_weekly → /v1/umbrella/top-identities
- **Top domains (ΔWoW)** → mart.top_domains_weekly → /v1/umbrella/top-domains
- **Early-warning** → mart.advanced_detections_weekly (+ allowed joins) → (surface in Top domains API or a dedicated endpoint)
- **Campaigns** → mart.domain_relation_weekly → (drawer/graph via Top domains item)

3) Detailed Analysis by Threat Vector — Developer Spec

Component

Tabbed drill-downs for **Malware**, **Phishing**, and **Command & Control (C2)**, each with KPI cards, leaders (Top domains/identities), and a context visualization (bar or geo). Tabs preserve tenant + week filters and reuse the same envelope response contract as the rest of the app.

Content (what each tab shows + how to build it)

3.1 Malware Analysis (tab)

- **KPIs:** Total Malware Blocks, ΔWoW, "Most Affected Identities" (Top 20). Computed from Umbrella Reports v2 filtered by threats=malware.
- **Leader table:** "Most Persistent Malware Domains" with **Investigate risk score** and WHOIS age. Data pull: Reports v2 destinations + Investigate risk/WHOIS on expand.
- **Viz:** Bar chart of top malware domains this week (WoW lollipops optional).

3.2 Phishing Analysis (tab)

- **KPIs:** Total Phishing Blocks, ΔWoW, "Users Who Clicked Most" (Top 20 impacted identities). Source: Reports v2 threats=phishing.
- **Leader table:** Top phishing destinations (domains) with Investigate risk band.
- **Viz:** Bar chart "Most common phishing domains".

3.3 C2 Analysis (tab)

- **KPIs:** Total C2 Blocks, ΔWoW, **Potentially Compromised Identities** (Top 20). Source: Reports v2 threats=commandandcontrol.
- **Leader table:** Top C2 destinations (domains). Enrich current resolving IPs → **geo map** of C2 server locations.
- **Viz:** World map (dest IP geolocated) with WoW "new/fast-rising infra" flags.

Shared deep-dive widgets (reused inside any tab):
A) Enriched Top-20 Malicious Domains (domain, threat_type, categories, risk_score, WHOIS age, ASN, ΔWoW, impacted_identities) with row expand → WHOIS, Related, Co-occurrence mini-graph. Ranking = 0.5·pct(risk) + 0.3·severity(threat) + 0.2·z(blocks); ties by identities then ΔWoW.
B) Early-Warning (newly-seen AND risk ≥ threshold AND allowed hits this week) with actions: simulate block / add to list / time-boxed exception.

Core Insight / Purpose

Move from totals to **vector-specific narratives**: which families/domains drive risk, which identities are most targeted, where the C2 infra sits, and **what to do now** per vector. This section ties destination context (Investigate) to block/allow evidence to make changes defensible.

Data model (read marts powering this section)

Use weekly "gold" marts (nightly) + current-week hourly refreshes where relevant. Keys follow (tenant_id, iso_year, iso_week, …).

- **Leaders & KPIs:**
  mart.top_domains_weekly (domain_sk, threat_family, blocks, rank, risk_rank) and
  mart.top_identities_weekly (identity_sk, blocks, risk_score, rank).
- **Trends/Heatmaps (optional inside tab):**
  mart.weekly_evolution_blocks, mart.heatmap_hourly_week.
- **Detections:**
  mart.advanced_detections_weekly (NEWLY_SEEN, DGA, FAST_FLUX, TUNNELING; top_examples JSONB).
- **Related graph:**
  mart.domain_relation_weekly (src_domain_sk, dst_domain_sk, edge_weight).

Time semantics: store **UTC**, present **Europe/Madrid**; ISO Week (Mon–Sun). Follow project enums (threat_family ∈ malware|phishing|commandandcontrol|…).

Public endpoints (read) + parameters

All list endpoints return { items, meta }, support **ETag/If-None-Match** (TTL 60–300s).

- GET /v1/umbrella/top-domains?tenant_id&iso_year&iso_week&limit=10&family=malware|phishing|commandandcontrol → leaders per vector.
- GET /v1/umbrella/top-identities?tenant_id&iso_year&iso_week&limit=20&family=… → “most affected” identities.
- GET /v1/umbrella/weekly-evolution?tenant_id&iso_year&iso_week&family=… → intra-week split for the tab trend.
- GET /v1/umbrella/heatmap?tenant_id&iso_year&iso_week&family=… → (optional) Hour×Day per vector.

Example response: /v1/umbrella/top-domains

```
{
 "items":[
  {
   "domain":"c2.badnet.tld",
   "family":"commandandcontrol",
   "blocks":1240,
   "delta_wow_pct":85.3,
   "risk_score":92.0,
   "asn_name":"AS13335",
   "asn_number":13335
  }
 ],
 "meta":{"count":10}
}
```

(ΔWoW computed server-side or by pairing current vs prior week.)

Calculations & server logic

- **ΔWoW** (domains/identities): (this_week - prev_week)/max(1, prev_week); expose as delta_wow_pct.
- **Ranking (Top domains):** 0.5·pct(risk_score) + 0.3·severity(family) + 0.2·z(blocks); ties by impacted_identities then ΔWoW.
- **Early-Warning rule:** is_newly_seen AND risk_score ≥ {tenant_threshold} AND allowed_hits_week > 0 (join Investigate + Reports v2 allowed).
- **Geo for C2:** resolve current IPs for domain and aggregate by country/ASN for the map; flag “new/fast-rising” when rank improves into Top-10 with strong ΔWoW.

UX wiring (Bubble)

- Tabs pass family to all calls; **tab switch preserves filters** (tenant, iso week).
- Leader tables: sortable by blocks and delta_wow_pct; row expand fetches Investigate detail (risk, WHOIS, related/co-occurrence).
- C2 tab: map markers show country/ASN and WoW label (“New”, “Fast-rising”).
- Early-Warning panel: inline actions for simulate-block / add-to-list / time-boxed exception.

Performance, freshness, retention

- **P95 latency:** < 500 ms for mart endpoints; < 1.5 s for heavy Top-N joins (limit 10).
- **Freshness:** facts hourly; weekly marts nightly; current-week trend/heatmap hourly.

- **Retention:** facts 90 days; marts 24 months (tenant-configurable).

Error & empty states

- **No data this week:** neutral placeholder + link to ingest/health. (Do not 500; return { items:[], meta:{count:0}}.)
- **Investigate rate-limit/outage:** render Umbrella-only fields and show **“stale Investigate”** badge on enriched cells. (Retry with backoff; respect ETag.)

Acceptance tests (traceable)

1. **Tabs**: switching Malware/Phishing/C2 keeps tenant/week; endpoints called with correct family.
2. **Leaders**: Top 10 domains/identities match mart.top_*_weekly; ΔWoW correct when prior=0 (guard with max(1, prev)).
3. **C2 Geo**: markers reflect aggregated dest IP geos; “new/fast-rising” label appears per rule.
4. **Enriched Top-20**: row expand shows risk, WHOIS age, ASN, related graph; ranking follows specified formula.
5. **Early-Warning**: only shows domains meeting all three conditions; action buttons trigger correct flows.

Quick lineage (widget → mart → endpoint)

- **Leaders (domains)** → mart.top_domains_weekly → /v1/umbrella/top-domains (with family) .
- **Leaders (identities)** → mart.top_identities_weekly → /v1/umbrella/top-identities.
- **Trend / intra-week** → mart.weekly_evolution_blocks → /v1/umbrella/weekly-evolution.
- **Heatmap (optional)** → mart.heatmap_hourly_week → /v1/umbrella/heatmap.
- **Detections / Early-Warning** → mart.advanced_detections_weekly (+ allowed joins).

3.1 Threats

Component

Top domains/identities for the current week, enriched with Investigate signals, ΔWoW, ASN/WHOIS, and action shortcuts (simulate/policy).

Content

- **Enriched Top 20 malicious domains** (domain, threat_type, categories, risk_score, WHOIS age, ASN, ΔWoW, impacted_identities) with row-expand to Investigate details and related/co-occurrence mini-graph; bulk select → "Add to Destination List."
- **Families/Campaigns** (cluster related domains via co-occurrence/related; one-click add family to list).

Core Insight / Purpose

Rank what truly matters this week, with enough adversary context to make **defensible policy changes** quickly.

Developer addenda (unchanged design)

Data model → marts

- mart.top_domains_weekly(tenant_id, iso_year, iso_week, domain_sk, threat_family, blocks, risk_rank, rank) for leaders.
- mart.top_identities_weekly(tenant_id, iso_year, iso_week, identity_sk, blocks, risk_score, rank) to derive **impacted_identities**.
- mart.domain_relation_weekly(tenant_id, iso_year, iso_week, src_domain_sk, dst_domain_sk, edge_weight) for related/co-occurrence graph.

Endpoints (read)

- GET /v1/umbrella/top-domains?tenant_id&iso_year&iso_week&limit=20&family=* (supports include=enrich to append Investigate fields).
- GET /v1/umbrella/top-identities?tenant_id&iso_year&iso_week&limit=20&family=* (for "impacted" joins).
  (All endpoints follow the public list & SLOs.)

Response contract (example, /v1/umbrella/top-domains)

```
{
 "items":[
  {
   "domain":"evil.example",
   "family":"commandandcontrol",
   "blocks":1240,
   "delta_wow_pct":85.3,
   "risk_score":92.0,
   "whois_created":"2025-07-02",
   "asn_name":"AS13335",
   "asn_number":13335,
   "impacted_identities":37
  }
 ],
 "meta":{"count":20}
}
```

Fields align with the Blueprint's "Enriched table" definition.

Server calculations

- **ΔWoW**: (this_week - prev_week)/max(1, prev_week) (guard divide-by-zero).

- **Ranking**: 0.5·pct(risk_score) + 0.3·severity(family) + 0.2·z(blocks); tie-break by impacted_identities then ΔWoW.

UX wiring (Bubble)

- Sortable by blocks / delta_wow_pct; chips for Threat Type/Categories/ASN; hover sparkline (7-day blocked vs allowed).
- Row-expand → Investigate panel; bulk-select → **Destination Lists** POST (chunk ≤500 entries).

SLOs & acceptance

- **P95**: <500ms for marts; <1.5s for Top-N (limit 10–20). **ETag** enabled.
- Tests: ΔWoW correct when prior=0; expand shows Investigate fields; family add-to-list chunks correct.

3.2 Investigate

Component

Detail panel for the **20 most-blocked** domains (weekly), surfacing **Risk/Status, Categories, WHOIS age, Related/Co-occurrence** and ASN.

Content

- **Risk & Status** (band + numeric), **Umbrella categories**, **WHOIS created / age**, **Related/Co-occurrence** ego-network, **ASN**.
- Drill-down modal tabs: Overview (KPIs+timeline), Network (related graph), WHOIS (current/history), DNS resolutions.

Core Insight / Purpose

Attach **actionable context** to each destination so SecOps can decide **block vs. exception** with evidence.

Developer addenda (unchanged design)

Delivery approach

- Primary grid comes from /v1/umbrella/top-domains. Add include=enrich=true to join Investigate (risk_score, whois_created, asn_*) and cache 24h; force refresh on row-expand.

Contract (added fields when include=enrich):
risk_score:number [0..100], risk_band:LOW|MED|HIGH, whois_created:date, asn_number:int, asn_name:string, related_preview:[{domain, score}].

Related graph

- Build from mart.domain_relation_weekly (co-occurrence/related); show top 10 neighbors by edge_weight; CTA “Add related to list”.

Acceptance

- Risk band matches numeric; WHOIS age flags <30 days; related graph shows ≥1 neighbor when present; cache refreshes on expand.

3.3 DNS Tunneling / DNS Abuse Detection

Component

A focused detector for **exfiltration or C2 over DNS**, combining **query-type mix**, **hourly periodicity**, and optional **subdomain entropy** signals; triage cards per identity.

Content

- **Signals**:
  - **Query-type spikes** in **TXT/NULL/AAAA** vs 4-week baseline (z-score) using Top DNS Query Types.
  - **Hourly heatmap** (identity × day × hour) to spot beaconing.
  - **NXDOMAIN spikes** (optional) and **subdomain length/entropy** if raw DNS is available.
- **Triage panel**: card per identity → %TXT, %NULL, z_score, “View recent destinations”; click reveals latest queries and Investigate risk for involved domains.

Core Insight / Purpose

Surface **stealthy data movement / beaconing** early and tie it to identities and destinations for fast containment.

Developer addenda (unchanged design)

Data model → marts

- mart.advanced_detections_weekly with detection ∈ {TUNNELING}; fields: count_domains, count_identities, top_examples JSONB.
- mart.heatmap_hourly_week(tenant_id, iso_year, iso_week, dow, hour, threat_family) for the Hour×Day visualization.

Endpoints (read)

- GET /v1/umbrella/heatmap?tenant_id&iso_year&iso_week&family=* (visual).
- **Add** GET /v1/umbrella/dns-tunneling?tenant_id&iso_year&iso_week&limit=20 → triage cards per identity from advanced_detections_weekly(top_examples) + computed ratios. (If you prefer not to add a route, return the detector block under /v1/umbrella/weekly-evolution as a named section.)

Response contract (example, /v1/umbrella/dns-tunneling)

```
{
 "items":[
  {
   "identity_id":"u:42",
   "pct_txt":46.2,
   "pct_null":12.1,
   "z_score_txt":3.4,
   "nxdomain_ratio":0.28,
   "examples":[{"domain":"exfil.bad.tld","count":312}],
   "mitre":["T1071.004"]
  }
 ],
 "meta":{"count":12}
}
```

Calculations

- Baseline: 4-week rolling mean/std per identity; z_score = (this_week - μ) / σ.
- “Suspect” if z_score_txt ≥ 2 **or** %TXT + %NULL ≥ tenant_threshold.

UX wiring

- Triage cards list; click opens identity drawer with recent queries and Investigate risk; heatmap filters by identity.

MITRE tag

- Label detections with **T1071.004 (DNS)** for exec reporting.

SLOs & acceptance

- SLOs per backend spec (P95 < 500ms marts).
- Tests: z-scores reproducible vs baseline; cards show examples from JSONB; heatmap re-filters within 200ms.

3.4 MITRE ATT&CK Mapping & Control Coverage

Component

A weekly ATT&CK view that maps volumes by technique (e.g., **T1566 Phishing**, **T1071.004 DNS C2**), and shows **which Umbrella/SWG policies actually fired** vs. **gaps** (allowed traffic).

Content

- **Technique mapping** table and heat cells (technique × volume/identities).
- **Control coverage**: for each technique, list policy hits (Malware/C2/Newly Seen, etc.) and highlight gaps (e.g., allowed Newly Seen + high risk). Back-links to policy simulation.

Core Insight / Purpose

Translate telemetry into a **common language** for execs and auditors and make **coverage gaps** explicit.

Developer addenda (unchanged design)

Implementation

- Maintain a static mapping {threat_type → [ATT&CK techniques]} as meta config; aggregate weekly events by threat_type and render the technique grid.
- Option A (new route): GET /v1/umbrella/mitre-weekly?tenant_id&iso_year&iso_week.
- Option B (reuse): return as an **insight** via GET /v1/ai/insights?tenant_id&iso_year&iso_week&kind=MITRE_MAP.

Response contract (example)

```
{
 "items":[
  {
   "technique":"T1566",
   "label":"Phishing",
   "events":2315,
   "unique_identities":174,
   "policies_fired":["Phishing","Newly Seen"],
   "coverage_gap_allowed":123
  },
  {
   "technique":"T1071.004",
   "label":"C2 over DNS",
   "events":890,
   "unique_identities":42,
   "policies_fired":["C2"],
   "coverage_gap_allowed":17
  }
 ],
 "meta":{"tenant_id":"...","iso_year":2025,"iso_week":33}
}
```

Data sources

- Weekly threat volumes & identities: existing **marts** (top domains/identities, evolution).
- Mapping & coverage join: static map + policy categories that fired, and allowed counts (for “gaps”).

Acceptance

- Techniques shown match mapping; volumes reconcile with weekly sums; **coverage_gap_allowed** equals allowed events for mapped threats; policy back-links open correct filtered views.

Global SLOs (apply to all above)

- **Latency:** P95 <500ms for marts; <1.5s for heavy Top-N.
- **Freshness:** facts hourly; marts nightly; current-week heatmap/trend hourly.
- **Retention:** facts 90d; marts 24m; per-tenant configurable.

4. Identity & Access Risk

Component
Focuses on user, device, and business-unit behavior as the core of risk. It consolidates Umbrella identity telemetry, weekly rollups, and AI signals into a single leaderboard + drill-downs.

Content

- **Identity Risk Ranking (leaderboard)**
  Table columns: Identity, Risk Score (0–100), Total Blocks, Highest Risk Category, Shadow-IT Apps Used. Source data is the weekly mart of top identities and CASB/Shadow-IT marts. Primary read is /v1/umbrella/top-identities.

- **Unified Identity Profile (drill-down)**
  Shows name/label, risk score, last 10 security blocks, top web categories (pie), cloud apps used. Base telemetry from Reporting v2 (activity by identity) and our weekly marts; profile aggregates appear in the drill-down view.

- **Security Event Timeline**
  Chronological log of significant blocks for the selected user/device; include DNS/SWG/CDFW where available.

- **Risky Behavior Summary**
  Top malicious domains, risky SWG URLs, blocked CDFW connections for that identity.

- **AI-driven Recommendations**
  Natural-language actions tied to the identity's pattern (e.g., "targeted phishing training"). Served by /v1/ai/recommendations.

- **Composite Risk Leaderboard / Statistical Outliers**
  Sortable list by composite score; highlight identities with z-score anomalies vs 13-week baseline.

- **DNS Tunneling Indicators (per-identity)**
  Widget tracks TXT/NULL/AAAA ratios and NXDOMAIN spikes vs 4-week average (Top DNS Query Types), flagged in the identity card.

- **Identity Distribution & Coverage**
  Distribution by identity type (site/roaming/AD user) and silent devices / client versions for coverage views. Umbrella identity distribution endpoints back the pie/stacked charts.

Core Insight / Purpose
Quantifies and prioritizes risk at the identity level using multi-factor signals (volume, severity, Shadow-IT, anomalies) and flags behaviors that policy rules might miss.

4.1 Data Model & Lineage (RAW → CORE → MART)

- **RAW (bronze):**
  raw_dns_activity, raw_identities, raw_casb_app_usage populated by hourly ingests; idempotent upsert keyed by (tenant_id, natural_id) with _hash.

- **CORE (silver):**
  Dimensions & daily facts that normalize Umbrella identities, domains, categories and counts; used for weekly builds and drill-downs (SCD2 on identities).

- **MARTS (gold, weekly):**
  - mart.top_identities_weekly(tenant_id, iso_year, iso_week, identity_sk, blocks, risk_score, rank) → powers the Identity Risk Ranking. Indexed by (tenant_id, iso_year, iso_week, blocks DESC, identity_sk).
  - mart.shadowit_flags_weekly, mart.shadowit_top_apps_weekly → used to augment "Shadow-IT Apps Used".
  - Other marts (KPIs, heatmap, trends) are joinable by (tenant_id, iso_year, iso_week) to back timeline and context.

- **AI Layer:**
  Baselines (mean/std/p50/p90/p99), anomaly flags ($z \geq 3$, >p99), and insights/recommendations persisted in ai.* tables; linked back to identities.

- **Indexing & Retention:**
  Weekly marts retained 24 months; facts 90 days; BRIN on time buckets; composite keys on (tenant_id, iso_year, iso_week) for report joins.

4.2 Backend Endpoints (Bubble-friendly)

- **Leaderboard:**
  GET /v1/umbrella/top-identities?tenant_id&iso_year&iso_week&limit=20&page=1
  Contract: list envelope with pagination + ETag caching.

- **AI Recommendations / Insights (identity-scoped via filter):**
  GET /v1/ai/recommendations?tenant_id&from&to&identity_id (optional filter) and GET /v1/ai/insights?... for anomaly badges.

- **Related reads used by the drill-down (reuse existing):**
  - GET /v1/umbrella/weekly-evolution?tenant_id&iso_year&iso_week&identity_id (filter param recommended)
  - GET /v1/umbrella/top-domains?tenant_id&iso_year&iso_week&identity_id&limit=10
  - GET /v1/shadow-it/top-apps?tenant_id&iso_year&iso_week&identity_id
    (Filters align with the catalog; the public list is in Appendix A.)

Standard list response envelope (all endpoints):

```
{ "items": [...], "meta": { "count": 123, "page": 1, "page_size": 20, "next": 2 } }
```

Use ETag/If-None-Match and TTL 60–300s.

4.3 Response Contracts (examples)

- **/v1/umbrella/top-identities → items[]**

```
{
  "identity_id": "8c7e3c8b-...",
  "identity_label": "user1@company.com",
  "identity_type": "roaming_user",
  "business_unit": "Finance",
  "blocks": 412,
  "risk_score": 92.4,
  "highest_risk_category": "phishing",
  "shadowit_high_risk_apps": 3,
  "rank": 1,
  "badges": { "anomalous": true, "dns_tunnel_suspected": true }
}
```

Backed by mart.top_identities_weekly (+ joins to CASB marts and AI flags).

- **Identity drill-down (composed payload)**

```
{
  "identity": {
    "id": "8c7e3c8b-...",
    "label": "user1@company.com",
    "type": "roaming_user",
    "risk_score": 92.4
  },
  "timeline": [
    { "ts": "2025-08-12T09:41:00Z", "family": "phishing", "domain": "login-secure-mail[.]com", "action": "blocked" }
  ],
  "top_categories": [{ "category": "Phishing", "pct": 46.1 }],
  "top_domains": [{ "domain": "malicious[.]xyz", "blocks": 87 }],
  "shadow_it": [{ "app": "Dropbox (personal)", "risk": "High", "users": 1 }],
```

"ai_recommendations": [{ "text": "Targeted phishing training for Finance." }]

}

Composition comes from weekly marts + AI tables and the same public endpoints listed in Appendix A.

4.4 Calculations & Scoring

- **Composite Identity Risk Score**
- risk_score = 100 * (
- w_vol * norm(blocks_this_week) +
- w_sev * avg(severity(threat_family)) +
- w_si * norm(#shadowit_high_risk_apps) +
- w_anom* clamp(z(blocks_by_identity, baseline_13w)/4, 0, 1)
-)

Defaults: w_vol=0.35, w_sev=0.25, w_si=0.20, w_anom=0.20.

  - norm(x) = min-max within tenant & week (use mart distribution).
  - severity(Malware|Phishing|C2|Cryptomining) map: 0.6/0.5/1.0/0.4 (tenant-tunable).
  - z(...) uses AI baselines from ai.baselines (13-week).

- **Anomaly Flag**: anomalous = (z ≥ 3) OR (blocks_p95_spike == true).
- **DNS Tunneling Suspect**: flag if pct_TXT ≥ p95_4w OR NXDOMAIN_rate ≥ p95_4w for the identity.

4.5 UX Wiring (Bubble)

- **Leaderboard RG** binds to /v1/umbrella/top-identities. Enable sort on risk_score (desc), blocks, filter by identity_type and business_unit. Row chips: type, BU, anomaly/tunnel badges. Click row → open drill-down group.
- **Drill-down** shows tabs: Overview (cards + sparkline), Timeline (table), Categories (pie), Apps (table), Recommendations (list). Same page; set a custom state identity_id for cross-widget filtering.
- **Empty/Skeleton states**: if meta.count==0, show guidance (“No telemetry this week for this identity type”). Use Bubble’s conditional rendering tied to API’s meta.

4.6 SLOs, Freshness & Pagination

- **Latency targets:** P95 < 500 ms for mart endpoints (leaderboard), P95 < 1.5 s for heavy toplists (page size ≤ 20). Use ETag and short TTLs.
- **Freshness:** Hourly ingests; current-week leaderboards refresh hourly; weekly marts materialized nightly.
- **Retention:** Facts 90 days; marts 24 months (tenant-configurable).

4.7 Security, Multitenancy & PII

- **Tenant guard** on every query; all marts keyed by tenant_id.
- **Secrets & rate limiting:** Rotate Umbrella/Investigate keys; throttle per tenant; circuit breaker on 429/5xx.
- **PII minimization:** Prefer identity labels from Umbrella; avoid storing emails beyond what’s returned; hash WHOIS emails from Investigate.

4.8 Acceptance Tests (traceable to UI)

- Leaderboard values equal mart.top_identities_weekly for (tenant_id, iso_year, iso_week); sort order by risk_score then blocks.
- Anomaly badges appear when z ≥ 3 in ai.insights; DNS tunneling badge toggles with TXT/NXDOMAIN thresholds.

- API contracts: list envelope keys present; ETag honored (304 on unchanged).
- UI parity with the sample weekly report layouts (leaderboard, cards, narrative).

4.9 Build Notes & SQL Sketch

- **Weekly job:** build_top_identities_weekly(tenant_id, iso_year, iso_week)
    - Aggregate weekly blocked counts by identity → join severity weights by threat family → left-join Shadow-IT counts → compute risk_score & rank → write to mart.top_identities_weekly. Indices: (tenant_id, iso_year, iso_week, blocks DESC, identity_sk).
- **AI baselines:** Recompute 13-week rolling stats per identity to power z and anomaly flags.

4.10 What the Developer Wires Up

1. Bind the leaderboard to /v1/umbrella/top-identities; pass tenant/week from the global filter bar.
2. On row click, set identity_id and load the drill-down widgets (timeline, categories, apps, recommendations) via the endpoints above.
3. Show badges using AI and DNS-type insights; tooltips display last-7-day sparkline from weekly evolution.

---

5. Application Visibility & Risk (Shadow IT & CASB)

Component

Application risk & adoption intelligence powered by Umbrella's **App Discovery** / CASB telemetry, surfaced as a bubble matrix + prioritised toplists and alert stream.

Content

- **Shadow IT Discovery** bubble chart (Risk × Compliance; bubble = users; color = overall risk).
- **KPIs**: total discovered apps, new this week, risk distribution.
- **Top 20 Very High/High-risk unreviewed apps** with action buttons.
- **Unsanctioned App Matrix** (Risk vs Usage).
- **Top Risky Apps** dashboard (users, sessions, data volume, sanction status).
- **Corporate vs Personal App Drift** (corp vs personal instances).
- **High-Risk Data Movement** (egress to file sharing/personal storage).
- **CASB Alerts** (exfil & policy violations).

Purpose

Expose **which cloud apps are in use, by whom, and how risky they are**, so security can block/monitor the right targets and compliance can govern data flows—using Umbrella as the sole telemetry source and the project's weekly marts for fast UI.

5.0 Cross-cutting Developer Notes (applies to all widgets)

- **Data source & cadence**: Ingest Umbrella CASB/App Discovery + SWG activity hourly into RAW, transform to CORE facts/dims, materialize **weekly marts** every night; current-week deltas recomputed hourly. Store in UTC, present in **Europe/Madrid**, ISO weeks (Mon–Sun). Retain facts 90 days, marts 24 months.
- **Table contracts (gold marts)** you'll read from:
  - mart.shadowit_flags_weekly — high-level flags (new high-risk apps, unsanctioned growth).
  - mart.shadowit_top_apps_weekly — per-app users/sessions/risk level (Top-N ready).
- **Public APIs (Xano)** mapped 1:1 to widgets:
  - GET /v1/shadow-it/flags
  - GET /v1/shadow-it/top-apps
    (ETag, pagination, TTL; multitenant guard).
- **Conventions**: schema families raw/core/mart/ai, enums (risk_level: LOW | MEDIUM | HIGH | CRITICAL), time semantics.
- **SLOs**: P95 < 500 ms for mart endpoints; ≤1.5 s for heavy Top-N (10–20).
- **UI parity**: match layout seen in the Weekly sample (CASB / Shadow IT section) and blueprint wording.

5.1 Shadow IT Discovery (Bubble Chart)

Component

Interactive bubble chart: **X** = vendor/business risk, **Y** = vendor compliance, **size** = users, **color** = risk.

Content

- Filters: time window (ISO week), business unit/site, risk bucket, sanction status.
- Tooltips: app name, users, sessions, data uploaded (MB/GB), risk level, compliance score.

Purpose

Prioritize unsanctioned apps where **business risk is high and compliance is low**, with large user footprint.

Developer spec

- **Endpoint**: GET /v1/shadow-it/top-apps?week=YYYY-Www&min_risk=HIGH&limit=200&group_by=app returns per-app aggregates for plotting. Backed by mart.shadowit_top_apps_weekly.
- **JSON (excerpt)**
- {
- "week": "2025-W33",
- "items": [
- {
- "app_id": "wetransfer_personal",
- "app_name": "WeTransfer (Personal)",
- "risk_level": "HIGH",
- "vendor_compliance_score": 42,
- "users_count": 28,
- "sessions": 311,
- "data_uploaded_mb": 4150,
- "sanction_status": "UNSANCTIONED"
- }
-],
- "etag": "W/\"d41d8c-...\""
- }
- **Data mapping**:
    - vendor_compliance_score and risk_level derive from Umbrella App Discovery metadata. Persist normalized ints 0–100 (compliance) and bucket risk into LOW/MEDIUM/HIGH/CRITICAL (CRITICAL → "Very High" in UI).
- **SQL sketch**:
    - users_count = COUNT(DISTINCT identity_sk); sessions = SUM(session_count); data_uploaded_mb = SUM(bytes_out) / 1048576.
- **Acceptance**: Risk/Compliance axes and bubble sizes must match weekly mart values within ±1%. (QA seeds from sample HTML "CASB / Shadow IT".)

5.2 Weekly KPIs (Header)

Component

KPI cards: **Total Discovered Apps**, **New This Week**, **Risk Distribution**.

Content

Numbers & mini-bars per risk bucket (Very High/High/Medium/Low).

Purpose

Give an at-a-glance **portfolio view** of app risk and weekly discovery velocity.

Developer spec

- **Endpoint**: GET /v1/shadow-it/flags?week=YYYY-Www (reads mart.shadowit_flags_weekly).
- **Calculations**:
    - new_this_week = COUNT(DISTINCT app_id WHERE first_seen_week = week)
    - risk_distribution[bucket] = COUNT(DISTINCT app_id WHERE risk_level=bucket)
- **UI**: map CRITICAL → "Very High" label.

5.3 Top 20 Very High-Risk Unreviewed Apps

Component

Prioritized table with **Action** buttons (e.g., “Create Block Policy”).

Content

Columns: Application, Risk, Users, DNS/SWG request volume, **AI Recommendation**.

Purpose

Fast path to **policying the worst offenders**.

Developer spec

- **Endpoint**: GET /v1/shadow-it/top-apps?week=YYYY-Www&risk=CRITICAL&reviewed=false&limit=20 (mart-backed).
- **AI Recommendations**: join with ai.recommendations_weekly on (tenant_id, iso_year, iso_week, app_sk) to show “Block/Monitor/Allow with Conditions”. (AI tables exist per blueprint.)
- **Action**: opens policy wizard (client-side route) prefilled with app_id + recommended control.

5.4 Top 20 High-Risk Unreviewed Apps

Component / Content / Purpose

Same as 5.3 but risk=HIGH. Keep the buttonized remediation flow.

Developer spec

- **Sorting**: ORDER BY users_count DESC, sessions DESC.
- **Empty-state**: show “All High-risk apps are already reviewed” with link to full list.

5.5 Unsanctioned App Matrix (Risk vs Usage)

Component

Quadrant chart (X: usage; Y: risk).

Content

Usage bands (Low/Med/High based on user quantiles) overlayed with risk buckets.

Purpose

Highlight **“High Risk / High Usage”** quadrant for immediate governance.

Developer spec

- **Endpoint**: same /v1/shadow-it/top-apps with include=usage_band.
- **Usage band**: compute weekly user count quantiles (33%/66%) per tenant → LOW/MED/HIGH. Persist in mart for deterministic UI.

5.6 Top Risky Apps Dashboard

Component

Table of unsanctioned **high-risk** apps with users, sessions, data volume, **sanction status** (Allowed/Blocked/Monitored).

Content

- Toggle “Include sanctioned apps” to benchmark policy coverage.
- Row-click → app drill-down: trend of users/sessions, identities list.

Purpose

Track **remediation progress** from “discovered” to “governed”.

Developer spec

- **Endpoint**: GET /v1/shadow-it/top-apps?risk=HIGH,CRITICAL&sanction_status=UNSANCTIONED&limit=50&page=N.
- **Drill-down**: GET /v1/shadow-it/app/:app_id/weekly-trend (derived from mart.shadowit_top_apps_weekly).

5.7 Corporate vs Personal App Drift

Component

Detector for **personal instances** of otherwise sanctioned apps (e.g., personal Gmail vs Workspace).

Content

Table: App, Drift Type (personal domain/OAuth scope), Users, Sessions, Data Uploaded, Suggested control.

Purpose

Reduce **data leakage & compliance risk** via shadow instances.

Developer spec

- **Logic** (mart build step): classify requests by **tenant-approved domains/SSO realms** vs **public domains**; mark drift=true when identity uses personal realm for a sanctioned app. Persist counts per week to mart.
- **Endpoint**: GET /v1/shadow-it/top-apps?drift=true.

5.8 High-Risk Data Movement

Component

Bar/stacked chart of outbound **bytes** to risky categories (File-Sharing, Personal Cloud, Webmail) + top contributing apps/URLs.

Content

Top 10 contributors; toggle by business unit/site.

Purpose

Reveal **where sensitive data might be going** and to which unsanctioned services.

Developer spec

- **Source**: SWG activity aggregated into mart; join to App Discovery classification.
- **Endpoint**: extend /v1/shadow-it/top-apps?metric=data_uploaded_mb.
- **Compute**: bytes_out rolled up by app + category per ISO week in mart.

5.9 CASB Alerts

Component

Critical alert list (exfiltration, policy breaches). Example: *“Detected file confidential_payroll.xlsx uploaded to a personal Dropbox account by user6.”*

Content

Columns: Time, Alert, Identity, App, Data Volume, Recommended Action.

Purpose

Operational feed for **immediate triage** of high-impact events.

Developer spec

- **Endpoint**: GET /v1/ai/insights?severity=HIGH,CRITICAL&topic=CASB&page=1&page_size=50 (re-use AI layer used elsewhere).
- **Backfill**: nightly AI job scans SWG/CASB facts to emit CASB insights into ai.insights_weekly.

5.10 Top 20 App Blocks by Policy

Component

Ranked list of apps **blocked** by Umbrella policies; shows which controls deliver value.

Content

Columns: App, Policy Name, Blocked Sessions, Identities Affected, ΔWoW.

Purpose

Demonstrate **control efficacy** in the application layer.

Developer spec

- **Source**: policy context available in SWG summaries; aggregate into mart.shadowit_top_apps_weekly with blocked_sessions.
- **Endpoint**: GET /v1/shadow-it/top-apps?verdict=blocked&limit=20.

5.11 Adoption Trend (“Tendencia de adopción”)

Component

Line/area trend of **users** and **sessions** per app (selectable).

Content

Week-over-week adoption to see if risk is growing or remediated after policying.

Purpose

Quantify **impact of governance actions**.

Developer spec

- **Endpoint**: GET /v1/shadow-it/app/:app_id/weekly-trend?weeks=12
- **Series**: users_count, sessions, data_uploaded_mb.
- **Policy markers**: overlay policy change events from Controls section (shared timeline).

5.12 UX, Caching, and Performance

- **Pagination**: all list endpoints page by page,page_size (default 25). Include total & next_page.
- **ETag/TTL**: compute ETag from (tenant_id, params, latest_updated_at); honor If-None-Match to 304. Suggested TTL: 10–15 min for current week.
- **SLOs**: P95 < 500 ms (marts) / < 1.5 s (heavy Top-N). Validate during acceptance.
- **RBAC**: Admin can see all orgs; Client sees only own org; User sees dashboards; enforce tenant_id middleware for every query.

5.13 Data Quality & Acceptance

- **DQ rules**:
  - users_count ≥ sessions_distinct_users sanity;
  - risk_level ∈ {LOW,MEDIUM,HIGH,CRITICAL};
  - Adoption trend continuity (no negative cumulative counts).
- **UI acceptance**:
  - Shadow-IT widget values align with **mart.shadowit_*** within tolerance;
  - Recommendations present for every row in Very High/High tables;
  - Bubble sizes and axes match numeric aggregates;
  - Sample section parity vs the Weekly HTML layout.

5.14 ERD & Marts (quick reference)

- **Marts used by Section 5**
  - mart.shadowit_flags_weekly(tenant_id, iso_year, iso_week, flags_total, high_risk_new, unsanctioned_increase)
  - mart.shadowit_top_apps_weekly(tenant_id, iso_year, iso_week, app_sk, users_count, sessions, risk_level, data_uploaded_mb, sanction_status, usage_band, drift)
  - Optionally link to mart.exec_delta_weekly for KPI deltas and to ai tables for recommendations.

Notes for Bubble Implementation

- Bind /v1/shadow-it/top-apps to the bubble chart and all Top-N tables; bind /v1/shadow-it/flags to KPI cards. Reuse the same binding patterns used elsewhere in Weekly pages (KPIs/Top lists).
- Follow the look-and-feel seen in the provided report HTML (card headers, table styles, risk badges).

6) SWG & CDFW Analysis (Unified Cloud Edge) — Developer Spec

Component

Two subviews: **SWG** (web security, TLS visibility, egress, UX) and **CDFW** (network firewall analytics & tunnel health).

Content

SWG

- Traffic Volume & Block Rate (Allowed vs Blocked trends; overall Block Rate %).
- TLS Inspection Dashboard (coverage %, bypass reasons, list of uninspected risky traffic).
- Data Egress by risky web categories (top URLs/apps).
- UX Telemetry (median/p95 request latency; outlier sites table).

CDFW

- Blocked Sessions by policy/port/protocol.
- Geo-Exposure map (src/dst for blocked traffic, anomalies).
- Top Talkers (identities/sites).
- Tunnel Health SLA (uptime %, latency, packet loss vs SLO).

Core Insight / Purpose

Balance **protection vs. enablement**: prove TLS visibility, spot risky egress, keep user experience healthy, and verify firewall coverage + tunnel reliability.

6.A Data model & lineage (RAW → CORE → MART)

Use UTC storage, ISO weeks, show times in **Europe/Madrid**. Weekly marts are the primary read surface; intra-week trend widgets read hourly rollups. SLOs/freshness from backend spec.

Existing "gold" marts used here

- mart.weekly_kpis_umbrella → block_rate_pct, tls_inspection_pct, cdfw_blocks.
- mart.nonsec_block_categories_weekly → category aggregates for egress & policy tables.

Add (small) supporting marts (keep same conventions)

- mart.swg_traffic_weekly(tenant_id, iso_year, iso_week, dow, allowed, blocked) – trend lines.
- mart.swg_tls_weekly(tenant_id, iso_year, iso_week, coverage_pct, bypass_reasons JSONB, risky_uninspected_top JSONB) – TLS coverage & bypass reasons (from SWG facts).
- mart.swg_latency_weekly(tenant_id, iso_year, iso_week, domain_sk, p50_ms, p95_ms, hits) – UX outliers.
- mart.cdfw_blocked_weekly(tenant_id, iso_year, iso_week, policy, dst_port, app_proto, count) – blocked by facets.
- mart.cdfw_geo_weekly(tenant_id, iso_year, iso_week, src_country, dst_country, sessions) – map.
- mart.tunnels_health_weekly(tenant_id, iso_year, iso_week, site, uptime_pct, latency_ms_p95, loss_pct_p95, sla_breaches) – SLA view.

Keep keys and weekly rollup patterns consistent with the catalog; index Top-N columns for P95 < 500 ms retrieval.

6.B Public endpoints (Bubble-friendly)

Use list envelope { items, meta }, **ETag/If-None-Match** (TTL 60–300s), and multitenant guard. See Appendix A list for related primitives (/kpis-weekly, /infra/status).

SWG

- GET /v1/umbrella/swg/traffic?tenant_id&iso_year&iso_week → trend (allowed/blocked by DOW) from mart.swg_traffic_weekly.
- GET /v1/umbrella/swg/tls-coverage?tenant_id&iso_year&iso_week → {coverage_pct, bypass_reasons[], risky_uninspected[]} from mart.swg_tls_weekly. (TLS% formula below.)

- GET /v1/umbrella/swg/egress?tenant_id&iso_year&iso_week&limit=10 → top risky categories + URLs/apps; join mart.nonsec_block_categories_weekly.

- GET /v1/umbrella/swg/latency-outliers?tenant_id&iso_year&iso_week&limit=20 → sites with highest p95 latency (from mart.swg_latency_weekly).

CDFW

- GET /v1/umbrella/cdfw/blocked-sessions?tenant_id&iso_year&iso_week&group_by=policy|dst_port|app_proto → bars & breakdowns (from mart.cdfw_blocked_weekly).

- GET /v1/umbrella/cdfw/geo-exposure?tenant_id&iso_year&iso_week → map points aggregating src_country,dst_country.

- GET /v1/umbrella/cdfw/top-talkers?tenant_id&iso_year&iso_week&limit=20 → identities/sites ranked by blocked sessions.

- GET /v1/umbrella/infra/status?tenant_id → connector/tunnel health primitives used in SLA view.

Sample contract (/v1/umbrella/swg/tls-coverage)

```
{
 "items":[
  {
   "coverage_pct": 78.6,
   "bypass_reasons":[{"reason":"CertError","pct":7.2},{"reason":"PolicyException","pct":5.1}],
   "risky_uninspected":[{"domain":"fileshare.example","hits":812}]
  }
 ],
 "meta":{"tenant_id":"...", "iso_year":2025, "iso_week":33}
}
```

6.C Calculations & server logic

- **Block Rate %** (weekly): security_blocks / total_requests. Source methodology confirmed in dev notes.

- **TLS Inspection %**: inspected_swg_requests / total_swg_requests. Provide **bypass reasons** breakdown based on SWG facts (e.g., cert error, explicit exception).

- **Data Egress (bytes)**: SUM(bytes_out) grouped by risky categories/apps; show Top-10 contributors.

- **UX Latency**: compute **p50/p95** per destination domain (or FQDN) using weekly window; flag outliers (p95 ≥ tenant threshold).

- **CDFW Blocked Sessions**: group by policy, dst_port, app_proto for breakdowns; **Top Talkers** rank by session count.

- **Tunnel Health SLA**: compare uptime_pct, latency_ms_p95, loss_pct_p95 against SLA thresholds; raise sla_breaches count and show red/amber/green.

6.D UX wiring (Bubble)

- Global filters (tenant, ISO week) drive both subviews. Tooltips include **definition + formula + data source** (explainability pattern).

- TLS panel: trend sparkline + coverage % + chip list of top bypass reasons; click “risky uninspected” → pre-filtered evidence view.

- CDFW map: click country pair → right drawer with sample flows & **policy** causing blocks.

- SLA widget: table grouped by site with badges; row click → /v1/umbrella/infra/status detail.

6.E Performance, freshness, retention, errors

- **P95** < 500 ms for mart endpoints; < 1.5 s for heavy Top-N. **Freshness:** hourly facts, nightly marts; current-week trends/heatmaps hourly. **Retention:** facts 90d; marts 24m.
- **Graceful degradation:** if TLS bypass reasons unavailable for a slice, show coverage% only and mark “data partial”.
- **Empty states:** “No egress to risky categories this week” / “No blocked sessions for selected facet”.

6.F Acceptance tests

1. TLS coverage equals mart.weekly_kpis_umbrella.tls_inspection_pct; bypass reasons sum to (100%−coverage%±1%).
2. Traffic trend = weekly sums by DOW; block rate matches method.
3. Egress Top-10 matches category aggregates; numbers reconcile to totals in KPI.
4. CDFW breakdowns facet correctly; **Top Talkers** sort stable; SLA breaches rendered red with evidence links.

---

7) Controls Efficacy & Deployment Hygiene — Developer Spec

Component

A health & efficacy section answering **“Are controls everywhere, and do they work?”** It includes coverage KPIs, a **Control Efficacy Funnel**, **What-if Policy Simulation**, **Policy Impact Analysis**, plus **Infrastructure & Licensing**.

Content

- **Deployment Coverage & Health**: “% identities reporting (7d)”, “% agents with SWG OK”, RAG by BU/site (Roaming Client status, last sync, client versions). Data: Deployments/RC.
- **Control Efficacy Funnel**: total requests → policy hits → **security overrides** (securityoverridden=true) → **noise filtered** (filternoisydomains=true).
- **What-if Policy Simulation**: model **Risk ≥ 80** or **Newly Seen** blocks over this week’s **allowed** traffic; estimate FPs.
- **Policy Impact Analysis (timeline overlay)** with “New Policy” markers (see sample weekly report Section 7).
- **Infrastructure & Licensing**: connector/tunnel status, license utilization, feature enablement checklist.

Core Insight / Purpose

Prove **coverage** and **effectiveness**, and safely preview the **impact** of potential policy changes before enforcing them.

7.A Data model & lineage

Existing marts powering 7.x

- mart.weekly_kpis_umbrella → agent_coverage_pct, tls_inspection_pct, global KPIs.
- mart.rc_outdated_weekly → outdated vs total clients + coverage %.
- mart.policy_simulation_weekly(simulation_key, would_block_count, fp_risk_estimate, top_examples) → What-if results.
- mart.exec_delta_weekly → KPI deltas/WoW for diff views.

Infra primitives come via /v1/umbrella/infra/status and /v1/umbrella/rc/outdated.

7.B Backend endpoints (read)

- **Coverage & Health**
  - GET /v1/umbrella/rc/outdated?tenant_id&iso_year&iso_week → {outdated_clients, total_clients, coverage_pct}.
  - GET /v1/umbrella/kpis-weekly?tenant_id&iso_year&iso_week → coverage/TLS/GRI etc.
- **Control Efficacy Funnel** *(new route)*
  - GET /v1/umbrella/controls-funnel?tenant_id&iso_year&iso_week → stages and drop-offs.
- **What-if Policy Simulation**
  - GET /v1/umbrella/policy-simulation?tenant_id&iso_year&iso_week&sim=RISK_GE_80|NEWLY_SEEN → reads mart.policy_simulation_weekly.
- **Policy Impact Overlay**
  - Reuse /v1/umbrella/trend-critical-4w plus a small policy-events feed (Xano table policy_events) to render vertical markers (as in sample Section 7 chart).
- **Infrastructure & Licensing**
  - GET /v1/umbrella/infra/status?tenant_id → connectors & tunnels heartbeat/errors.
  - (Optional) GET /v1/umbrella/licensing?tenant_id → seats, assigned, active, expiry.

Standard list response

{ "items":[...], "meta": { "tenant_id":"...", "iso_year":2025, "iso_week":33 } }

7.C Contracts (examples)

/v1/umbrella/controls-funnel

```
{
 "items":[
   {
     "total_requests": 12834567,
     "policy_hits": 2314567,
     "security_overrides": 12450,
     "noise_filtered": 315000
   }
 ],
 "meta": {"tenant_id":"...", "iso_year":2025, "iso_week":33}
}
```

(“policy_hits” covers security + content policies; “security_overrides” uses securityoverridden=true; “noise_filtered” uses filternoisydomains=true.)

/v1/umbrella/policy-simulation?sim=RISK_GE_80

```
{
 "items":[
   {
     "simulation_key":"RISK_GE_80",
     "would_block_count": 187432,
     "fp_risk_estimate": 0.06,
     "top_examples":[{"domain":"young-ecom.tld","allowed_hits":412,"risk_score":91}]
   }
 ],
 "meta":{"iso_year":2025,"iso_week":33}
}
```

Backed by mart.policy_simulation_weekly.

/v1/umbrella/rc/outdated

```
{
 "items":[{"outdated_clients": 84, "total_clients": 1320, "coverage_pct": 93.6}],
 "meta":{"iso_year":2025,"iso_week":33}
}
```

7.D Calculations & logic

- **% identities reporting (7d)**: distinct identities with any telemetry in last 7 days / identities licensed.
- **% agents with SWG OK**: active agents with healthy SWG state / total agents. (From RC + SIG status.)
- **Control Efficacy Funnel**:
    - total_requests: all DNS+SWG requests this week.
    - policy_hits: requests with any policy match (security/content).
    - security_overrides: subset with securityoverridden=true.
    - noise_filtered: volume removed by “noisy domain” filter for clarity.

- **What-if sims**: join **allowed** requests with Investigate signals and apply predicate (e.g., risk_score ≥ 80 or domain ∈ NewlySeen). Compute would_block_count, basic **FP estimate** using historic allow→benign ratio for same category/tenant. Persist as mart.policy_simulation_weekly.
- **Policy Impact Analysis**: overlay policy_events.ts over blocked-trend series; display immediate Δ on block rate (see sample chart).

7.E UX wiring (Bubble)

- Coverage RAG by BU/site: traffic-light cells with tooltips (definition + source).
- Funnel: stacked bars per stage; click any stage → pre-filtered evidence (deep link).
- What-if: dropdown to switch **RISK ≥ 80** vs **Newly Seen** simulations; show **Top examples** with one-click "simulate → blocklist draft" flow.
- Policy Impact: line chart with vertical **policy markers** (title, author). Matches the sample weekly section 7 pattern.
- Infra & Licensing: status table + gauges + enablement checklist (SWG, CDFW, CASB, Investigate).

7.F Performance, freshness, retention, errors

- **P95** < 500 ms (marts), < 1.5 s (Top-N/sims). **Freshness:** hourly facts; nightly sims/materializations. **Retention:** facts 90d; marts 24m (per-tenant configurable).
- **Graceful degradation**: if Investigate unavailable, show simulation results with a **"stale enrich"** badge and omit FP estimate for that slice.

7.G Acceptance tests (traceable)

1. Coverage tiles equal mart.weekly_kpis_umbrella.agent_coverage_pct and mart.rc_outdated_weekly.coverage_pct.
2. Funnel stages reconcile to request totals with expected monotonic drop.
3. What-if results match mart.policy_simulation_weekly and are reproducible ±5% vs recompute.
4. Policy Impact overlays render markers and show a measurable post-change Δ (see weekly Section 7 example).
5. Infra/Licensing pulls from /infra/status and shows feature-enablement checklist items.

7.H Security, tenancy, and ops

- Every endpoint enforced by tenant guard; **ETag/TTL** for list routes; secrets rotated; rate-limit per tenant; audit "policy simulation viewed/exported".

Handy cross-references (widget → mart → endpoint)

- **TLS Coverage** → mart.weekly_kpis_umbrella.tls_inspection_pct + mart.swg_tls_weekly → /v1/umbrella/swg/tls-coverage.
- **Egress Top-10** → mart.nonsec_block_categories_weekly → /v1/umbrella/swg/egress.
- **CDFW Blocks** → mart.cdfw_blocked_weekly → /v1/umbrella/cdfw/blocked-sessions.
- **Coverage KPIs** → mart.weekly_kpis_umbrella + mart.rc_outdated_weekly → /v1/umbrella/kpis-weekly, /v1/umbrella/rc/outdated.
- **What-if** → mart.policy_simulation_weekly → /v1/umbrella/policy-simulation.
- **Policy Impact** → trend endpoints + policy_events (overlay like sample HTML).

---

8) Advanced Operational Visualizations — Developer Spec

Component

Rich, interactive diagrams for analysts to visualize **flows and composition** beyond standard tables: **Sankey (Identity → Threat Category → Verdict)** and **Sunburst (Security Category → Destination Domains)**.

Content

- **Sankey**: identity → threat category → blocked/allowed verdict (weekly).
- **Sunburst**: hierarchical breakdown from security category into destination domains (Top-N).
  Purpose is to expose risk paths and multi-dimensional relationships that are hard to see in flat lists.

Core Insight / Purpose

Provide intuitive, multi-dimensional views so analysts can **see where risk originates, how it propagates, and where controls intervene**.

8.A Data lineage & marts (RAW → CORE → MART)

- **Source facts**: Umbrella Reports v2 (top destinations, summaries by category/destination, verdicts) hydrated into CORE dims (identity/domain/category).
- **Gold marts (weekly)**
  - mart.flow_identity_category_verdict_weekly(tenant_id, iso_year, iso_week, identity_sk, category_sk, verdict, count) → **Sankey** links.
  - mart.sunburst_category_domain_weekly(tenant_id, iso_year, iso_week, category_sk, domain_sk, count) → **Sunburst** nodes.
  - Both marts built nightly; current-week refresh hourly for deltas. Keys follow (tenant_id, iso_year, iso_week, …).

Retention & indexing: marts 24m; facts 90d; composite indexes on (tenant_id, iso_year, iso_week) and Top-N columns for P95 < 500 ms.

8.B Public endpoints (Bubble-friendly)

All return the standard list envelope { items, meta }, honor **ETag/If-None-Match** (TTL 60–300s), and enforce row-level tenancy.

1. **Sankey**
   GET /v1/vis/sankey?tenant_id&iso_year&iso_week&min_flow=50&max_nodes=80
   Response (d3-compatible):

```
{
  "items": [{
    "nodes": [
      {"id":"id:user42","label":"user42@org"},
      {"id":"cat:phishing","label":"Phishing"},
      {"id":"v:block","label":"Blocked"}
    ],
    "links": [
      {"source":"id:user42","target":"cat:phishing","value":312},
      {"source":"cat:phishing","target":"v:block","value":290}
    ]
  }],
  "meta":{"tenant_id":"...", "iso_year":2025, "iso_week":33}
}
```

Derived from mart.flow_identity_category_verdict_weekly. min_flow prunes edges; max_nodes caps layout cost.

2. **Sunburst**
   GET /v1/vis/sunburst?tenant_id&iso_year&iso_week&limit_per_category=25
   Response (hierarchical):

```
{
 "items":[
  {"name":"Security Categories","children":[
   {"name":"Phishing","children":[{"name":"auth-login-mail[.]com","value":512}]},
   {"name":"C2","children":[{"name":"badc2.tld","value":207}]}
  ]}
 ],
 "meta":{"tenant_id":"...","iso_year":2025,"iso_week":33}
}
```

Built from mart.sunburst_category_domain_weekly (Top-N per category).

8.C Calculations & rules

- **Verdict mapping**: Normalize to blocked|allowed from Reports v2 verdicts before aggregating flows.
- **Top-N pruning**: Rank domains per category by weekly count; keep N via limit_per_category; aggregate “Other” for completeness (sum must reconcile).
- **PII minimization**: Option to pseudonymize identity labels in Sankey (hash(identity_sk)), switchable per tenant setting.

8.D UX wiring (Bubble)

- **Sankey**: node click opens right-drawer with **frozen evidence** (identity-filtered threats or category slice). **Link click** deep-links to verdict slice.
- **Sunburst**: ring click filters Top Destinations table pre-scoped to that category.
- Tooltips show **definition + formula + source** per Blueprint convention.

8.E Performance & freshness

P95 < 500 ms for mart reads; fail-soft for over-dense graphs by auto-raising min_flow and showing “graph pruned” notice. Hourly refresh for current-week; nightly for historical.

8.F Acceptance tests

1. Sankey totals equal weekly sums (within ±1% after pruning “Other”).
2. Sunburst totals per category reconcile with the weekly category summary.
3. Deep-links open with tenant/week filters frozen.
4. ETag honored (304 on unchanged).

---

9) Prioritized Recommendations & Remediation — Developer Spec

Component

Turn insights into a **weekly, owner-driven plan**: a **Prioritized Action Table** with **evidence links**, **Policy Diff View**, **Event Correlation**, **Predictive Analysis**, and **Benchmarking**.

Content

- **Prioritized Action Table** (sortable/filterable): columns **Recommendation, Priority, Impact, Effort, Owner, ETA, Status**, plus **Evidence Link(s)** back to the exact filtered views. UI mirrors the Weekly report style.
- **Policy "Diff View"**: before/after impact for a chosen change window.
- **Event Correlation**: narrative that ties spikes to assets/apps (e.g., TrickBot + legacy server + risky RDP).
- **Predictive Analysis**: Talos-informed forward risk joined to local exposure (outdated software).
- **Benchmarking**: industry-anonymized deltas (conceptual).

Core Insight / Purpose

From "what we saw" to **"what we'll do, who owns it, when it will be done, and how we prove the impact."**

9.A Data model (AI + marts)

- **AI tables (governed layer)**:
  ai.recommendations(reco_id, tenant_id, iso_year, iso_week, title, body, priority, impact, effort, owner, eta, status, evidence_links JSONB, tags JSONB);
  ai.insights(insight_id, kind, severity, narrative, evidence_links JSONB);
  ai.playbooks(playbook_id, key, action_steps JSONB);
  ai.weekly_exec (for leadership narrative).
- **Diffs & benchmarks (small marts)**:
  mart.policy_diff_weekly(tenant_id, policy_key, window_start, window_end, pre_blocks, post_blocks, pre_allow, post_allow, delta_pct, top_examples JSONB);
  mart.industry_benchmarks_weekly(naics2, metric_key, p50, p75, p90) (optional).

Cadence: nightly population; recommendations update when AI jobs run; "Diff View" recomputed on-demand and cached (ETag).

9.B Backend endpoints (public)

- GET /v1/ai/recommendations?tenant_id&iso_year&iso_week&status=*&priority=* → table feed.
- GET /v1/ai/recommendations/:reco_id → full record + playbook.
- GET /v1/ai/policy-diff?tenant_id&policy_key&from&to → pre/post metrics + top examples.
- GET /v1/ai/correlation?tenant_id&iso_year&iso_week → event correlations (insights).
- GET /v1/ai/benchmarks?tenant_id&industry=* (optional).
  All endpoints use the list envelope & ETag; row-level tenant guard.

Example contract — /v1/ai/recommendations

```
{
 "items":[
  {
   "reco_id":"reco-8f7a",
   "title":"Block domain auth-m365-portal.net across all policies",
   "priority":"High",
   "impact":"High",
   "effort":"Low",
   "owner":"IT Security",
   "eta":"2025-08-23",
      "status":"Not Started",
      "evidence_links":[
        "/threats?family=phishing&week=2025-W33&domain=auth-m365-portal.net"
      ],
      "tags":["phishing","policy"]
    }
  ],
  "meta":{"tenant_id":"...","iso_year":2025,"iso_week":33}
}
```

Matches the blueprint’s table columns and the sample weekly report visuals.

Example contract — /v1/ai/policy-diff

```
{
  "items":[
    {
      "policy_key":"block_newly_seen",
      "window_start":"2025-08-12",
      "window_end":"2025-08-18",
      "pre_blocks":12400,
      "post_blocks":620,
      "pre_allow":8900,
      "post_allow":210,
      "delta_pct":-95.0,
      "top_examples":[{"domain":"fresh-reg.tld","pre_hits":540,"post_hits":7}]
    }
  ],
  "meta":{"tenant_id":"..."}
}
```

Implements the **“Diff View”** example in the Blueprint.

9.C Calculations & scoring

- **Priority score** (server):
  priority_score = 0.5·impact + 0.3·likelihood + 0.2·urgency, mapped to **Critical/High/Medium** for display; default likelihood from recent hit rate; urgency from SLA/asset criticality.
- **Effort** heuristic: small/medium/large from playbook step count & required roles.
- **Diff View**: compute **pre/post** over tenant-chosen window; show relative %Δ and absolute deltas; provide Top examples.
- **Event correlation**: join spikes (e.g., C2) to identities/assets and risky apps within same window; output narrative + evidence deep-links.
- **Predictive analysis**: ingest Talos signal (campaign/exploit), intersect with **local exposure** (e.g., outdated software list) and emit recommendation with **Predictive Risk** flag.
- **Benchmarking**: compare tenant metrics (e.g., phishing block rate, high-risk Shadow IT count) to anonymized industry quartiles where available.

9.D UX wiring (Bubble)

- **Action table**: sortable by **Priority**, **Impact**, **ETA**; row expand shows **playbook steps** and **Diff View** sparkline; “Open evidence” uses deep-link URLs from the record.
- **Create from insight**: “Promote to Recommendation” button on insight cards; pre-fills Owner/ETA and links evidence.
- **Status changes**: client toggles (Not Started/In Progress/Done) via PATCH endpoint (optional future).
  UI style matches the weekly report section for continuity.

9.E Performance, freshness, retention

- **P95** < 500 ms for list reads; < 1.5 s for policy-diff compute (cache by param hash).
- **Freshness**: Recommendations/insights nightly; manual refresh allowed on drawer open.
- **Retention**: AI tables 24m; diffs retained for 6m (recomputable).

9.F Acceptance tests (traceable)

1. Every recommendation has **≥1 evidence link** resolving to a valid filtered view.
2. **Diff View** reproduces pre/post counts within ±5% of recompute for the same window.
3. **Correlation** narratives cite the concrete assets/apps and provide links.
4. **Predictive** items include a Talos reference token (or cached signal) and list the exposed assets.
5. Table columns and statuses match the Blueprint definition verbatim.

9.G Example records (seed)

- **Critical**: “Isolate SRV-DATA-01 due to C2 traffic; run forensic scan.” Owner: **SOC**; ETA: **48h**; Evidence: C2 trend + identity logs (links).
- **High**: “Block auth-m365-portal.net in all policies.” Owner: **IT Sec**; Evidence: Top Phishing Domains + Investigate risk.
- **Medium**: “Update 60 outdated agents.” Owner: **IT Ops**; Evidence: RC Outdated report. (Matches weekly sample.)

Quick cross-map (widget → mart/AI → endpoint)

- **Action Table** → ai.recommendations → /v1/ai/recommendations.
- **Diff View** → mart.policy_diff_weekly (or on-demand compute) → /v1/ai/policy-diff.
- **Correlation** → ai.insights → /v1/ai/correlation.
- **Benchmark** → mart.industry_benchmarks_weekly → /v1/ai/benchmarks (optional).

---

10) Incidents & Response — Developer Spec

Component

An **incident queue + SLA tracker** built from Umbrella detections, enriched with Investigate, and prioritized with opinionated rules (**P1**, **Q2**). Includes MTTD/MTTR trends and an **Incident Detail** with timeline, related identities/assets, and evidence links.

Content

- **Prioritization**
  - **P1**: C2 or High Risk (≥90) from privileged identities/servers.
  - **Q2**: Newly-Seen + Allowed + recent WHOIS.
- **SLA & Throughput**: MTTD/MTTR lines, % incidents meeting SLA, backlog & aging. (Weekly sample shows MTTD/MTTR + “Incident SLA Met”.)
- **Incident Detail**: title, severity, owner, status, start/end, detection rule, impacted identities, top evidence (domains/ASNs), policy hits/misses, remediation notes.

Core Insight / Purpose

Turn noisy detections into **work you can close**—clearly prioritized, SLA-tracked, with evidence and impact.

10.A Data lineage (RAW → CORE → MART/IR)

- **RAW**: raw_dns_activity, raw_cdfw_events, raw_inv_* as already defined.
- **Correlation job (hourly)**: cluster detections by *(tenant, identity/device, destination/family, 6–24h window)*, dedupe with a suppression window; tag with rule keys (P1_C2_PRIV, Q2_NEWLYSEEN_ALLOWED, etc.).
- **Gold / IR marts** (weekly):
  - mart.ir_incidents_weekly(tenant_id, iso_year, iso_week, incident_id, severity, rule_key, opened_at, closed_at, mttd_s, mttr_s, sla_met, owner, status)
  - mart.ir_incident_entities(tenant_id, incident_id, identity_sk, asset_label)
  - mart.ir_evidence(tenant_id, incident_id, domain_sk, category_sk, blocked, allowed, risk_score)
  - mart.ir_sla_weekly(tenant_id, iso_year, iso_week, mttd_hours, mttr_hours, sla_met_pct, backlog_open, backlog_aging_days_p95)
- **Cadence/retention**: facts hourly; marts nightly; **facts 90d**, **marts 24m**.

10.B Backend endpoints (Bubble-ready)

Use list envelope + **ETag/If-None-Match** (TTL 60–300s) and tenant guard. Follow the public API patterns in the Backend Spec.

- GET /v1/ir/incidents?tenant_id&iso_year&iso_week&severity=*&rule_key=*&status=*
  → rows from mart.ir_incidents_weekly (+ join owner display).
- GET /v1/ir/incidents/:incident_id
  → incident header + entities[] + evidence[] (+ top examples).
- GET /v1/ir/sla?tenant_id&iso_year&iso_week
  → {mttd_hours, mttr_hours, sla_met_pct, backlog_open, backlog_aging_days_p95} from mart.ir_sla_weekly.
- (Optional) POST /v1/ir/incidents/promote → create an incident from an AI insight/domain slice (stores linkage to ai.insights).

Response shape (examples)
/v1/ir/incidents

```
{
 "items":[
  {
   "incident_id":"inc_2025W33_014",
   "title":"C2 activity from SRV-DATA-01",
   "severity":"P1",
   "rule_key":"P1_C2_PRIV",
   "opened_at":"2025-08-13T07:42:11Z",
   "closed_at":null,
   "owner":"SOC Tier2",
   "status":"Open",
   "mttd_s":900,
   "mttr_s":null,
   "sla_met":false
  }
 ],
 "meta":{"tenant_id":"...","iso_year":2025,"iso_week":33}
}
```

/v1/ir/sla

```
{
  "items":[{"mttd_hours":2.5,"mttr_hours":12.8,"sla_met_pct":82.0,"backlog_open":7,"backlog_aging_days_p95":4}],
  "meta":{"tenant_id":"...","iso_year":2025,"iso_week":33}
}
```

(Values mirror the weekly sample charts/tiles.)

10.C Rules & calculations (server)

- **Severity**
  - **P1** if (threat_family=C2 **OR** risk_score ≥ 90) **AND** identity.is_privileged=true **OR** asset.role IN ('server','dc').
  - **Q2** if is_newly_seen=true **AND** allowed_hits>0 **AND** whois_age_days < 30.
- **MTTD** = opened_at - first_detection_at; **MTTR** = closed_at - opened_at.
- **SLA Met**: compare MTTD/MTTR to tenant SLA thresholds; expose % met. (Dashboard shows “Incident SLA Met”.)
- **Evidence selection**: Top domain_sk by blocked/allowed counts + Investigate risk_score; attach ASN & categories.

10.D UX wiring (Bubble)

- **Incidents table**: severity pill (P1/Q2), age, owner; filters by rule/severity/status.
- **Detail drawer**: tabs—Overview (SLA, times, owner), Evidence (domains, categories, risk), Entities (identities/assets), Timeline (detections, actions).
- **Links**: “Open evidence” deep-links to pre-filtered threats/identity views; “Promote to Recommendation” for long-tail mitigations. (Pattern reused from Sections 8–9.)

10.E Performance, freshness, errors

- **SLOs**: P95 < 500 ms for mart reads; < 1.5 s for heavy detail joins. **Freshness**: hourly facts; nightly marts; current-week recompute hourly. **Retention**: 90d/24m.
- **Graceful degradation**: If Investigate enrichment is stale, show badge “Enrichment T-24h” and suppress WHOIS-age gating for Q2.

10.F Acceptance tests

1. **P1/Q2** classification matches rule table for curated test fixtures.
2. **MTTD/MTTR** reconcile with opened_at/closed_at in mart.ir_incidents_weekly and match chart tiles.

3. **SLA %** equals sla_met aggregation across incidents per week.
4. Evidence links resolve to filtered threat/identity pages; counts reconcile ±1% with source marts.

11) Appendix — Developer Spec

Component

Reference compendium for formulas, enums, field dictionary, time conventions, known limitations, and ops SLOs.

Content

- **Methodology**: composite risk, KPIs, and detection rules.
- **Field dictionary**: API contracts & mart columns.
- **Known limitations**: Umbrella scope; optional enrich (Investigate, ticketing).
- **Ops**: performance, freshness, retention, indexing, caching, tenancy & security.

Core Insight / Purpose

Make the dashboard **auditable and reproducible**—definitions are explicit and traceable from UI → API → mart → source.

11.A KPI & metric formulas (authoritative)

- **Block Rate %** = security_blocks / total_requests.
- **TLS Inspection %** = inspected_swg_requests / total_swg_requests.
- **Agent Coverage %** = active_agents_last7d / licensed_agents.
- **Incident SLA %** = % of incidents where (MTTD≤SLA_Detect AND MTTR≤SLA_Remediate). (Shown in Executive.)
- **Global Risk Index (GRI)** = weighted composite of *threat severity*, *identity risk*, *Shadow-IT exposure* (weights documented in code comments).
- **Identity Risk Score** example = 0.5·percentile(InvestigateRisk) + 0.3·weight(threatType) + 0.2·zscore(blocks_per_identity).
- **DNS Tunneling z-score**: compute %TXT, %NULL per identity vs 4-week baseline; flag z>2.

11.B Prioritization rules (reference)

- **P1**: (family=C2 OR risk_score≥90) AND (identity.privileged OR asset in {server,dc}).
- **Q2**: newly_seen=true AND allowed_hits>0 AND whois_age<30d.
  These keys (“rule_key”) are persisted with each incident for auditability.

11.C Time, cadence, retention

- **Timezone**: store UTC; render **Europe/Madrid**; ISO week keys.
- **Cadence**: facts hourly; **weekly marts nightly**; current-week deltas hourly.
- **Retention**: facts **90 days**; marts **24 months** (per-tenant).

11.D Field dictionary (selected)

- **mart.ir_incidents_weekly**:
  incident_id (PK), tenant_id, iso_year, iso_week, severity (P1|Q2|P2|P3), rule_key, opened_at, closed_at, owner, status (Open|Contained|Resolved|FP), mttd_s, mttr_s, sla_met (bool).
- **mart.ir_sla_weekly**: mttd_hours, mttr_hours, sla_met_pct, backlog_open, backlog_aging_days_p95.
- **API list envelope**: { items:[], meta:{count,page,page_size,next} }, with **ETag**.

11.E Non-functional & ops

- **Performance**: P95 <500 ms (marts), <1.5 s (heavy Top-N/detail).

- **Indexing**: BRIN on time in high-volume facts; composite (tenant_id, iso_year, iso_week) on marts; dims unique on natural keys.
- **Caching**: ETag from (tenant_id, params, latest_updated_at); TTL 60–300s; 304 on unchanged.
- **Tenancy & security**: every table keyed by tenant_id; middleware guard; secrets in env; audit audit_api_calls.

11.F Known limitations

- **Scope**: Cisco Umbrella is the authoritative telemetry. Some visuals (e.g., MTTD/MTTR, SLA) improve with optional ticketing integration (Jira/ServiceNow) but can be computed locally from incident lifecycle when tickets are absent.
- **Investigate quotas**: batch POST up to 1000 domains; respect rate limits; cache 24h.

11.G Acceptance (auditability)

- Every widget cites its **formula + source** in tooltip; numbers reconcile from UI → API → mart with tolerance in Backend Spec acceptance.
