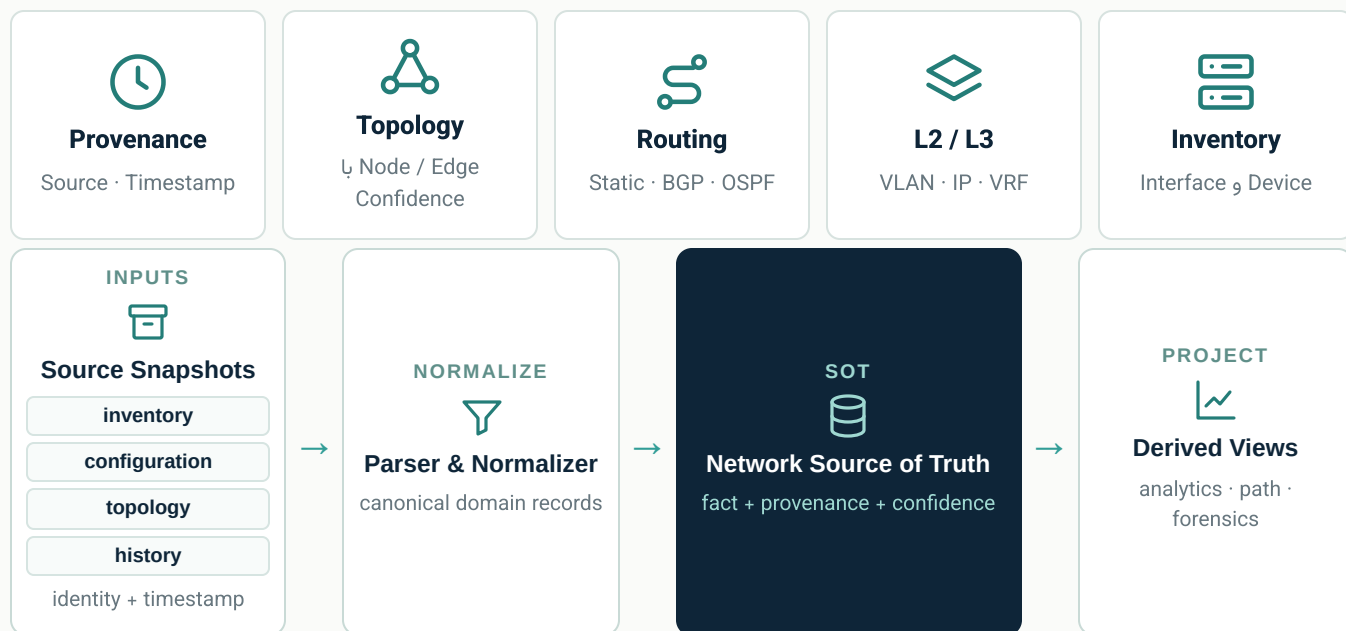


4SO Network

بروشور فنی

Network Source of Truth with Provenance & Confidence

اطلاعات پراکنده‌ی شبکه را به یک مدل ماشین‌خوان تبدیل می‌کند؛
Routing، L2/L3، Interface، Inventory، توپولوژی و History با منشأ
مشخص نگهداری می‌شوند و Inference هرگز بی‌صدا به Fact تبدیل
نمی‌شود.



Projection ≠ Authority

forensics و Summary، path view روی رکوردهای منبع ساخته می‌شوند و مرجع دوم نمی‌سازند.

Inference بی‌صدا Fact نمی‌شود

رابطه‌ای که فقط از Naming یا Diagram به دست آمده تا Corroboration در وضعیت Candidate می‌ماند.

شبکه را به داده‌ای تبدیل کنید که می‌دانید چقدر می‌شود به آن اعتماد کرد.

CAPABILITY SNAPSHOT

Capability Snapshot

داده‌های شبکه به دامنه‌های قابل تحلیل شکسته می‌شوند

هدف، تبدیل Config dump به یک مدل عملیاتی است که بتوان روی آن Query، Correlation و Forensics انجام داد.



VRF و IP

Routing Context و Addressing



Port-channel و VLAN

Segment، Membership و Aggregation



Interface Model

Interface، Description و Bundle



Device Inventory

مدل ساخت‌یافته مستقل از فرمت Source



History و Provenance

Change و Timestamp، Source history



Service Dependencies

Logging و DNS، Time، AAA



Topology

Node/Edge با Source و Confidence



Routing Facts

Static، BGP و OSPF برای تحلیل مسیر

اصول عملیاتی



Config خام دارای Secret وارد خروجی نمی‌شود



Confidence از Provenance جدا نمی‌شود



Diff تغییر را نشان می‌دهد، نه علت را



بدون فرمان روی دستگاه یا تغییر Config زنده

مرز مالکیت داده



Fact پیکربندی به Snapshot همان Source تعلق دارد



Fact توپولوژی به منبع Diagram خودش تعلق دارد



رابطه‌ی Candidate تا Corroboration قطعی نیست



Derived view فقط Projection است

Source Snapshot → Parse → Normalize → Correlate → Classify → Review → Derived :Core contract

View — هر مرحله راه برگشت به Source را حفظ می‌کند.



Authority Model

منبع مهم است؛ میزان اطمینان هم همین‌طور

به‌جای یک جدول Flat که همه‌چیز را Truth قطعی فرض کند، داده بر اساس منشأ و روش استخراج طبقه‌بندی می‌شود.

DERIVED
Summary، مسیر یا تحلیل روی
رکوردهای منبع؛ مرجع دوم ایجاد نمی‌کند.
projection · reproducible

CANDIDATE
استنباط از Naming، Description یا
Diagram؛ با Confidence و روش
استنباط ثبت می‌شود.
bounded inference · confidence

FACT
آنچه Source واقعاً گفته؛ فقط در
محدوده‌ی همان Snapshot و
Timestamp معتبر است.
source-scoped · timestamped

SYNTHETIC RECORD SHAPES

FACT
domain interface
source config snapshot
observed timestamp
class fact

CANDIDATE
domain link
method description match
confidence bounded
state needs review

DERIVED
domain path view
inputs L2 · L3 · routing
lineage source manifest
authority none

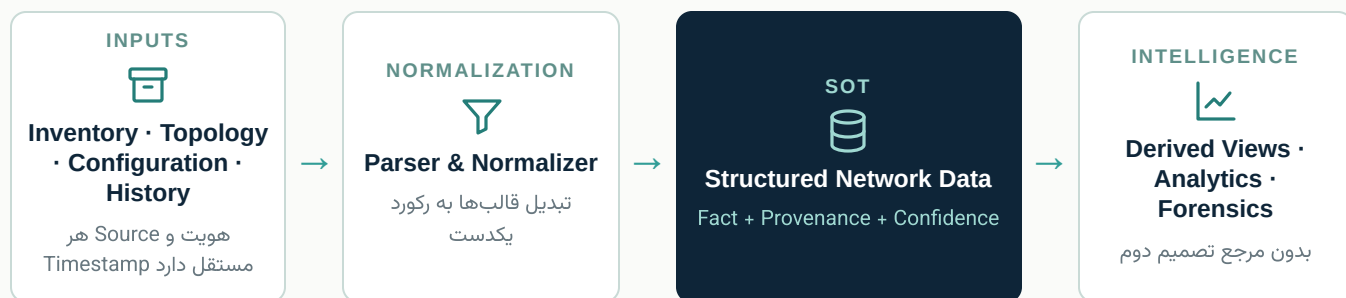
کاربرد	Authority / Confidence	رکوردهای نمونه	Domain
normalization و Inventory	Fact در محدوده‌ی Snapshot	Device identity, platform/role, source mapping	Inventory
تحلیل Link-layer	Config-derived + timestamp	Interface, VLAN, port-channel	Interfaces / L2
تحلیل مسیر و Policy	رکورد مشاهده‌شده یا config-derived	IP/subnet, VRF, static, BGP, OSPF	L3 / Routing
Inference بدون تبدیل Truth به Correlation	Derived Candidate Fact	Node, Edge, link candidate	Topology
تحلیل وابستگی سرویس	رابطه‌ی Source-owned یا استنباط محدود	DNS, Time, AAA, Logging	Dependencies
Forensics و مقایسه	Timestamp + provenance	Snapshot identity, change context	History

ARCHITECTURE OVERVIEW

Architecture Overview

Pipeline باید Provenance را حفظ کند، نه پاک

منابع جدا ingest می‌شوند، Parser آن‌ها را Normalize می‌کند و مرجع واحد داده رکوردها را با منشأ و Confidence نگه می‌دارد.



نوع Evidence	Classification	قاعده‌ی استفاده
Configuration snapshot	Fact در محدوده‌ی Snapshot	فقط با Source و Timestamp خودش معتبر است
Topology / diagram	Source-scoped fact	رابطه در Diagram اثبات وضعیت زنده‌ی شبکه نیست
Naming / description	Candidate	Link، Role یا Site استنباطی پیش از Corroboration قطعی نمی‌شود
Multi-source	Confidence-bearing	منشأها و شواهد پشتیبان همراه رابطه می‌مانند
Derived view	Projection	از داده‌ی Source-owned ساخته می‌شود؛ SoT دوم نیست
Historical compare	Change context	تغییر را نشان می‌دهد؛ علت حادثه را بدون Evidence ادعا نمی‌کند



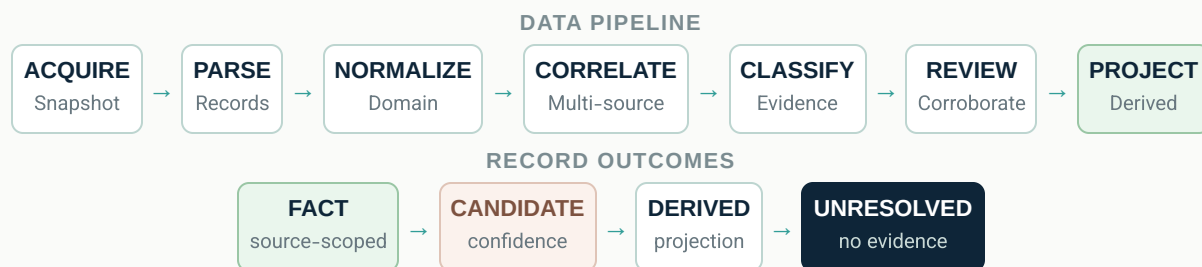
Correlation: رابطه‌ی ساخته‌شده از چند Source، Confidence، Timestamp و شواهد پشتیبان را همراه خود نگه می‌دارد؛ Correlation مالکیت Source را حذف نمی‌کند.

ACTION & WORKFLOW CONTRACT

Action & Workflow Contract

اکشن اصلی: تبدیل Evidence به مدل قابل تحلیل

این محصول تغییری روی شبکه‌ی زنده اعمال نمی‌کند؛ workflow اصلی مدیریت Evidence و Classification است.



Failure / Recovery	Success	Execution	Admission	Action
Parse ناموفق Source قبلی را overwrite نمی‌کند	هر رکورد به Snapshot قابل برگشت	Parser فقط داده‌ی همان Source	هویت، hash و timestamp منبع	Ingest Snapshot
Field مجهول جعل نمی‌شود	Source و Identity mapping حفظ شود	تبدیل به مدل canonical	Device، برای Parser Interface، L2/L3، Routing	Normalize
Conflict پنهان یا collapse نمی‌شود	Source‌های پشتیبان قابل نمایش	ساخت رابطه بدون حذف ownership	کلید match و provenance هر دو طرف	Correlate
بدون Corroboration به Authority نمی‌رسد	از Fact قابل تشخیص و قابل review	Candidate با Confidence و روش	Hint برای استنباط محدود	Infer Candidate
Unresolved = نبود شواهد	Classification با trace حفظ شود	ارزیابی با شواهد تکمیلی	Evidence مستقل یا تأیید اپراتور	Review
خروجی عمومی داده‌ی حساس را حذف می‌کند	Reproducible و بدون دوم SoT	Projection از رکوردهای موجود	Snapshot‌ها و Policy حساسیت	Export Safe View

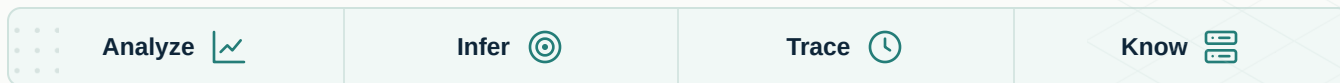
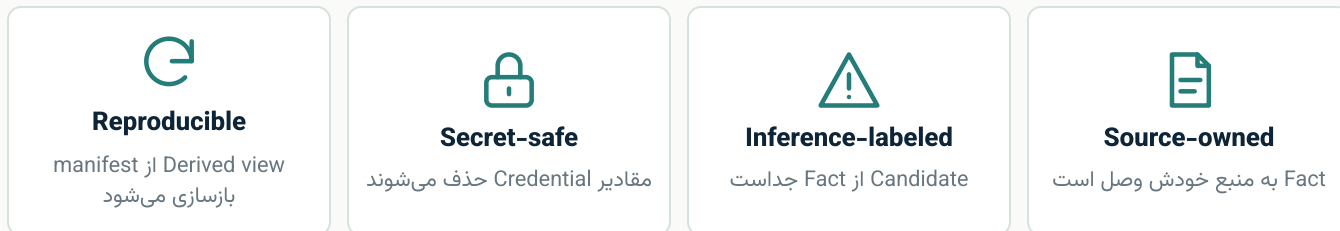
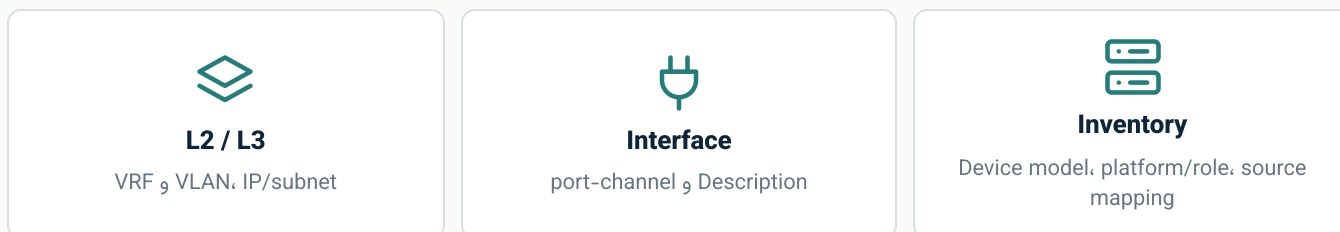
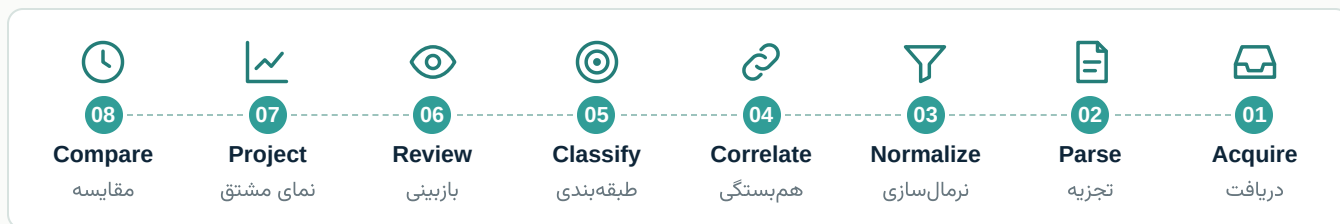
Projection ≠ Authority: Summary، path view، analytics یا forensics از چند Source ساخته می‌شود، اما Fact اصلی به Source و Timestamp خودش متصل می‌ماند.



Lifecycle & Data Profiles

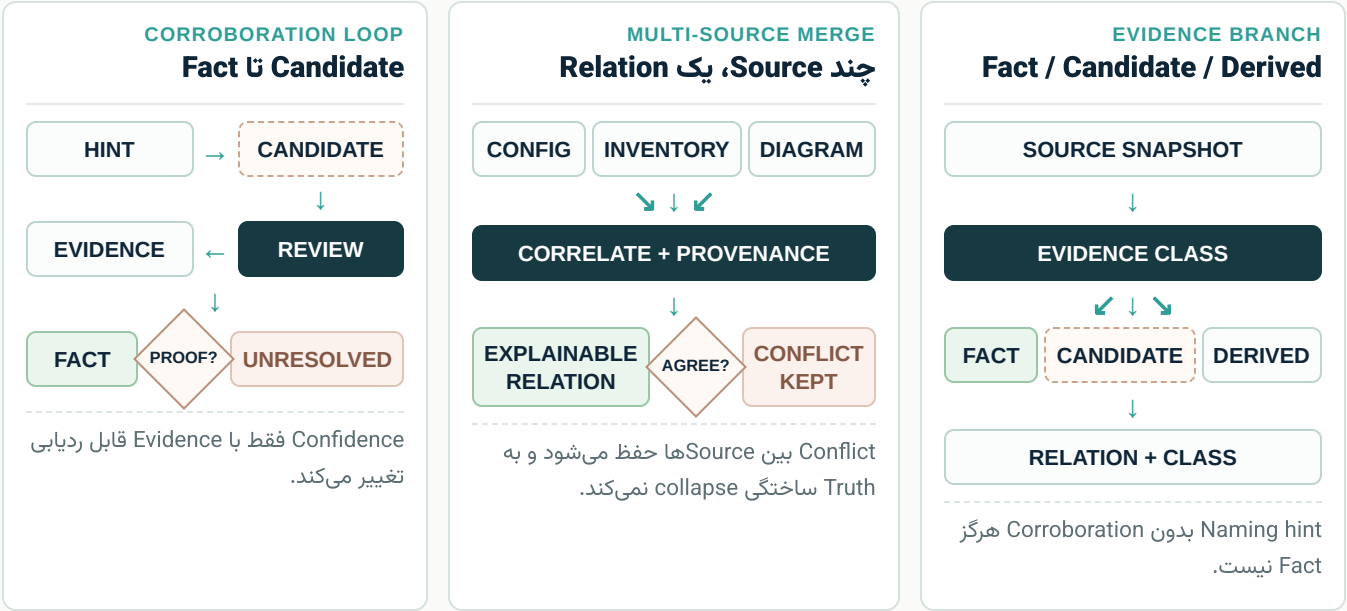
داده‌ی شبکه هم چرخه‌ی عمر کیفیت دارد

Snapshot تا زمانی که Parse، Classify و Correlate نشده فقط Raw Input است؛
Derived Result هم تا Review جای Fact را نمی‌گیرد.



Data-Quality Failure Semantics

ابهام باید دیده شود، نه پنهان



Recovery	Product Behavior	Detection	Failure Domain
دریافت Source تازه‌تر	Fact در محدوده‌ی همان Snapshot می‌ماند	Timestamp و History منبع	Stale snapshot
گسترش Parser و تولید دوباره	Field ناموجود، ناموجود می‌ماند	خطای Schema یا Parse	Parser gap
نگه‌داشتن Conflict و Evidence	برنده‌ی بی‌صدا انتخاب نمی‌شود	عدم تطابق در Correlation	Source conflict
Corroboration مستقل	به Fact ارتقا پیدا نمی‌کند	پایین Confidence	Weak inference
فقط Metadata می‌ماند	مقدار حذف می‌شود	تشخیص و Redaction	Sensitive content

Path analysis: اگر Evidence لینک یا Routing ناقص باشد Confidence کاهش می‌یابد؛ سیستم مسیر گمشده را جعل نمی‌کند.

Action & Operations Catalog

کاتالوگ عملیات، مهندسی داده برای شبکه است



Parse •

- L3
- L2
- interfaces
- devices
- routing



Acquire •

- verify manifest
- ingest snapshot
- history sync



Quality •

- conflict review
- classify
- secret redaction



Correlate •

- topology match
- device match
- link candidate



Forensics / Export •

- provenance trace
- snapshot diff
- safe summary



Analyze •

- routing view
- subnet view
- dependency view

Evidence و Observability |



تازگی داده از History و Timestamp



خطای Parse یک سیگنال کیفیت داده است



هر گزارش Derived با manifest قابل ردیابی

Sensitivity و Security |



مقادیر Credential از Dataset تولیدی حذف می‌شوند



یافته‌ی Secret فقط به صورت Metadata و redacted



Query و Export تابع Policy حساسیت

Action safety: کاتالوگ عملیات داده‌محور است؛ هیچ فرمان عمومی روی دستگاه یا تغییر پیکربندی زنده ادعا نمی‌شود.



داده‌ی شبکه‌ای که منشأ و میزان اعتمادش روشن است.

4SO Network برای تصمیم‌گیری روی داده‌های شبکه ساخته شده است؛ با Provenance و Confidence به عنوان بخشی از خود مدل.

