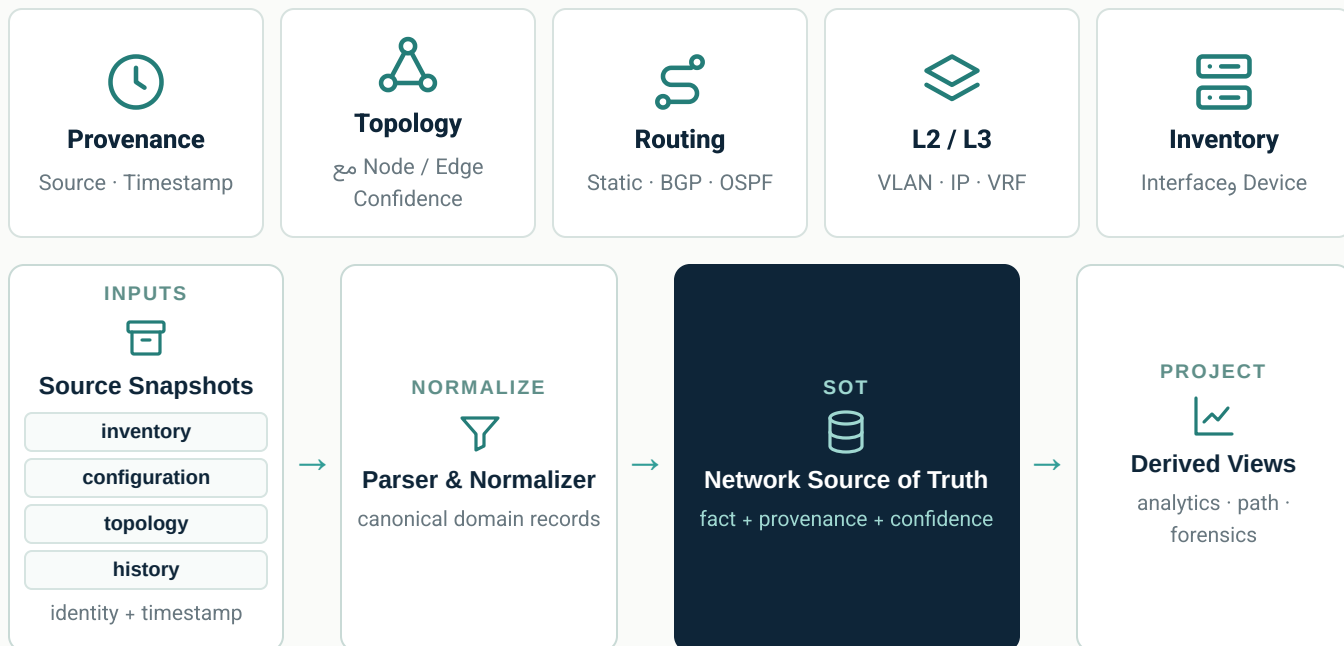


4SO Network

كتيب تقني

Network Source of Truth with Provenance & Confidence

يحوّل معلومات الشبكة المتناثرة إلى نموذج قابل للقراءة آلياً؛ إذ تُحفظ Inventory و Interface و L2/L3 و Routing والطوبولوجيا و History مع منشأ واضح، ولا يتحول Inference أبداً إلى Fact بصمت.



Projection ≠ Authority

تُبنى Summary و path view و forensics فوق سجلات المصدر، ولا تُنشئ مرجعاً ثانياً.

لا يتحول Inference إلى Fact بصمت

العلاقة المستخلصة من Naming أو Diagram فقط تبقى في حالة Candidate حتى تتم Corroboration.

حوّل الشبكة إلى بيانات تعرف تماماً إلى أي حدّ يمكن الوثوق بها.



CAPABILITY SNAPSHOT

Capability Snapshot

تُقسّم بيانات الشبكة إلى مجالات قابلة للتحليل

الهدف هو تحويل Config dump إلى نموذج تشغيلي يمكن إجراء Query و Correlation و Forensics عليه.



VRF و IP

Routing Context و Addressing



Port-channel و VLAN

Membership و Segment Aggregation



Interface Model

Description و Interface Bundle



Device Inventory

نموذج منظم مستقل عن صيغة Source



History و Provenance

Change و Source و Timestamp history



Service Dependencies

Logging و AAA و Time و DNS



Topology

Source مع Node/Edge Confidence



Routing Facts

Static و BGP و OSPF لتحليل المسار

مبادئ التشغيل



لا تدخل Config الخام المحتوية على Secret إلى المخرجات



لا تنفصل Confidence عن Provenance



يُظهر Diff التغيير، لا سببه



بلا أوامر على الأجهزة أو تغيير Config الحية

حدود ملكية البيانات



Fact الإعدادات تنتمي إلى Snapshot المصدر نفسه



Fact الطوبولوجيا تنتمي إلى مصدر Diagram الخاص بها



العلاقة Candidate ليست قاطعة قبل Corroboration



Derived view ليست سوى Projection

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

View – تحافظ كل مرحلة على طريق العودة إلى Source.



Authority Model

المصدر مهم، ومستوى الثقة كذلك

بدلاً من جدول Flat يفترض أن كل شيء Truth قاطعة، تُصنّف البيانات وفق منشئها وطريقة استخراجها.

DERIVED
Summary أو مسار أو تحليل فوق
سجلات المصدر؛ لا يُنشئ مرجعاً ثانياً.
projection · reproducible

CANDIDATE
استنتاج من Naming أو Description أو
Diagram؛ يُسجّل مع Confidence
وطريقة الاستنتاج.
bounded inference · confidence

FACT
ما قاله Source فعلاً؛ صالح فقط ضمن
نطاق Snapshot و Timestamp ذاتهما.
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

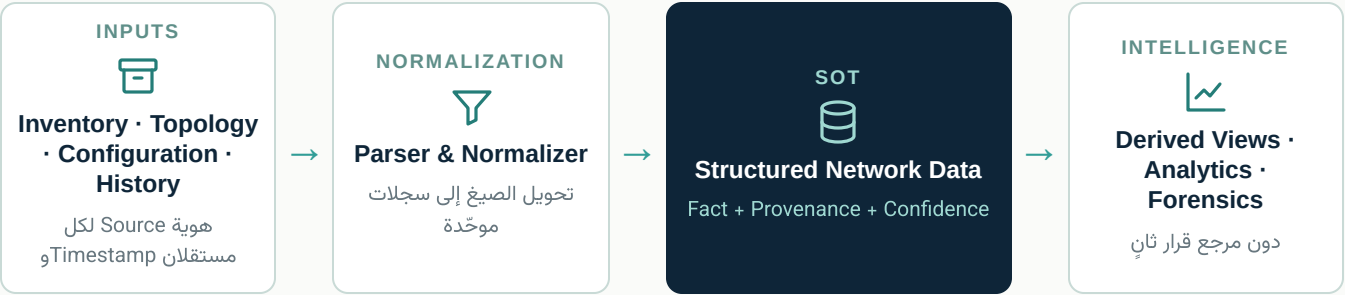
Domain	سجلات نموذجية	Authority / Confidence	الاستخدام
Inventory	source و platform/role و Device identity mapping	Fact ضمن نطاق Snapshot	normalization و Inventory
Interfaces / L2	port-channel و VLAN و Interface	Config-derived + timestamp	تحليل Link-layer
L3 / Routing	OSPF و BGP و static و VRF و IP/subnet	سجل مرصود أو config-derived	تحليل المسار و Policy
Topology	link candidate و Edge و Node	Derived Candidate Fact	Inference دون تحويل Truth إلى Correlation
Dependencies	Logging و AAA و Time و DNS	علاقة Source-owned أو استنتاج محدود	تحليل تبعيات الخدمة
History	change context و Snapshot identity	Timestamp + provenance	Forensics والمقارنة

ARCHITECTURE OVERVIEW

Architecture Overview

على Pipeline أن يحفظ Provenance، لا أن يمحوه

تُستوعَب المصادر (ingest) كلُّ على حدة، ويتولى Parser تطبيعها (Normalize)، ويحتفظ المرجع الموحد للبيانات بالسجلات مع منشئها وConfidence.



نوع Evidence	Classification	قاعدة الاستخدام
Configuration snapshot	Fact ضمن نطاق Snapshot	صالحة فقط مع Source وTimestamp الخاصين بها
Topology / diagram	Source-scoped fact	العلاقة في Diagram ليست إثباتاً للحالة الحية للشبكة
Naming / description	Candidate	لا يصبح Link أو Role أو Site المستنتج قاطعاً قبل Corroboration
Multi-source	Confidence-bearing	تبقى المصادر والأدلة الداعمة مقترنة بالعلاقة
Derived view	Projection	تُبنى من بيانات Source-owned؛ وليست SoT ثانية
Historical compare	Change context	تُظهر التغيير؛ ولا تدّعي سبب الحادثة دون Evidence

Ambiguity visible
لا يُخفى Conflict ولا Unknown

Secret-safe
تُحذف قيم Credential من Dataset

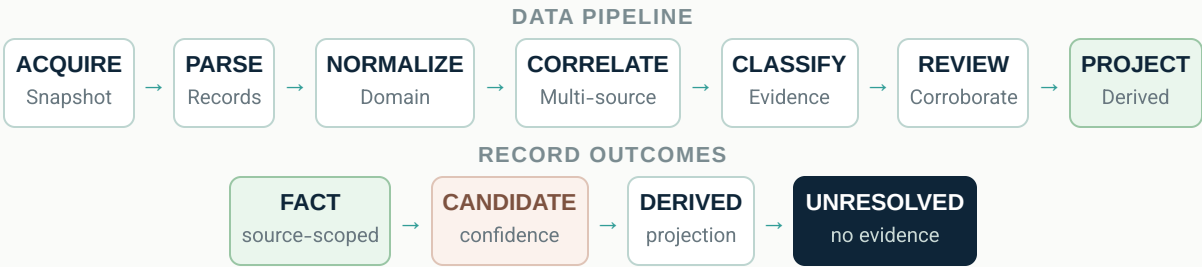
Reproducible
يعيد Parser وGenerator بناء المخرجات من manifest

Correlation: العلاقة المبنية من عدة Source تحمل معها هوية المصدر وTimestamp وConfidence والأدلة الداعمة؛ ولا تُلغي Correlation ملكية Source.

Action & Workflow Contract

الإجراء الأساسي: تحويل Evidence إلى نموذج قابل للتحليل

لا يطبق هذا المنتج أي تغيير على الشبكة الحية؛ ف workflow الأساسي هو إدارة Classification و Evidence.



Failure / Recovery	Success	Execution	Admission	Action
فشل Parse لا يكتب فوق Source السابق	كل سجل قابل للإرجاع إلى Snapshot	Parser يقرأ بيانات ذلك Source فقط	هوية المصدر و hash و timestamp	Ingest Snapshot
لا يُختلق Field مجهول	حفظ Source و Identity mapping	التحويل إلى النموذج canonical	Parser J Device و Interface و Routing و L2/L3	Normalize
لا يُخفى Conflict ولا يُدمج (collapse)	إمكان عرض المصادر الداعمة	بناء العلاقة دون إلغاء ownership	مفتاح match و provenance للطرفين	Correlate
لا يبلغ Authority دون Corroboration	قابل للتمييز عن Fact و قابل للمراجعة	Candidate مع Confidence والطريقة	Hint لاستنتاج محدود	Infer Candidate
Unresolved = غياب الأدلة	حفظ Classification مع trace	تقييم بأدلة إضافية	Evidence مستقلة أو تأكيد المشغل	Review
المخرجات العامة تحذف البيانات الحساسة	Reproducible و دون SoT ثانية	Projection من السجلات الموجودة	Snapshots وسياسة الحساسة	Export Safe View

Projection ≠ Authority: تُبنى Summary و path view و analytics و forensics من عدة مصادر، لكن Fact الأصلية تبقى مرتبطة ب Source و Timestamp الخاصين بها.



Lifecycle & Data Profiles

بيانات الشبكة أيضاً دورة حياة للجودة

تبقى Snapshot مجرد Raw Input ما لم تخضع ل Parse و Classify و Correlate، ولا يحلّ Derived Result محلّ Fact قبل Review.



L2 / L3
VRF و IP/subnet و VLAN

Interface
port-channel و Description

Inventory
source و platform/role و Device model mapping

Forensics
last-change context و Source history

Topology
link candidate و Device matching

Routing
OSPF و BGP و Static

Reproducible
يُعاد بناء view Derived من manifest

Secret-safe
تُحذف قيم Credential

Inference-labeled
Fact منفصلة عن Candidate

Source-owned
Fact مرتبطة بمصدرها

Analyze

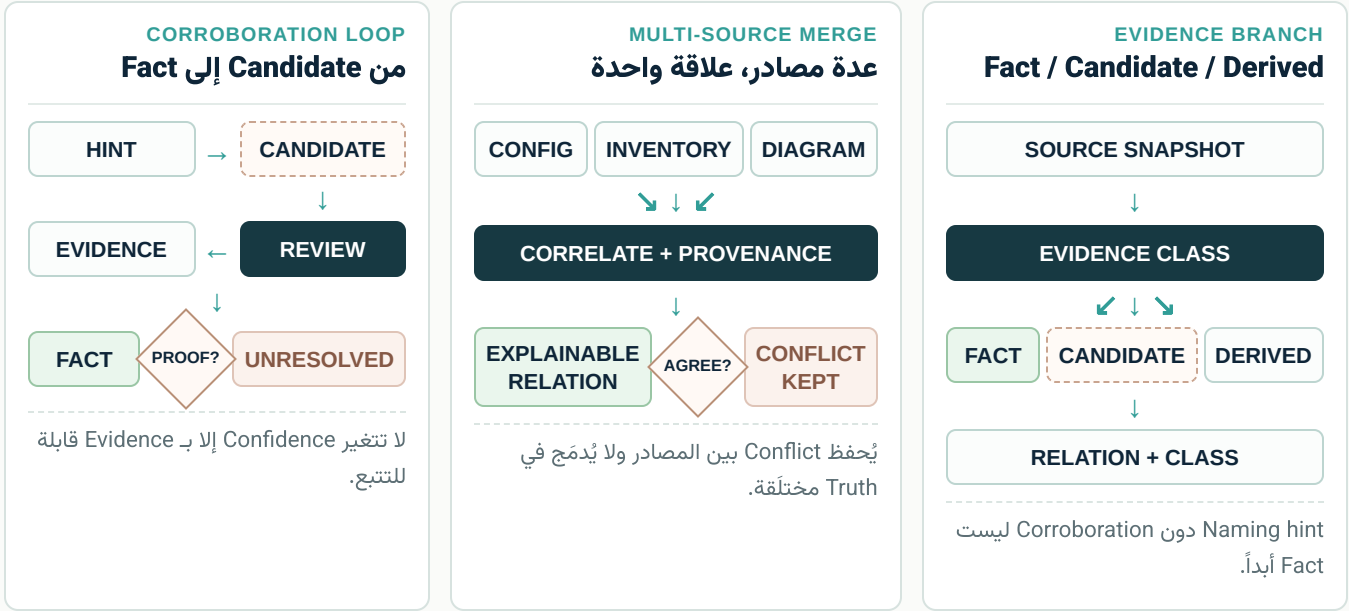
Infer

Trace

Know

Data-Quality Failure Semantics

يجب أن يكون الغموض ظاهراً، لا مخفياً



Recovery	Product Behavior	Detection	Failure Domain
استلام Source أحدث	تبقى Fact ضمن نطاق Snapshot ذاتها	Timestamp و History المصدر	Stale snapshot
توسيع Parser وإعادة التوليد	Field المفقود يبقى مفقوداً	خطأ Schema أو Parse	Parser gap
الإبقاء على Conflict و Evidence	لا يُختار فائز بصمت	عدم تطابق أثناء Correlation	Source conflict
Corroboration مستقلة	لا تُرقى إلى Fact	Confidence منخفضة	Weak inference
تبقى Metadata فقط	تُحذف القيمة	الكشف و Redaction	Sensitive content

Path analysis: إذا كانت Evidence الخاصة بالرباط أو Routing ناقصة تنخفض Confidence؛ ولا يخلق النظام المسار المفقود.

Action & Operations Catalog

كتالوج العمليات هو هندسة بيانات للشبكة



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 |



حداثة البيانات من History و Timestamp



خطأ Parse إشارة على جودة البيانات



كل تقرير Derived قابل للتتبع عبر manifest

Security والحساسية |



تُحذف قيم Credential من Dataset المولدة



اكتشافات Secret فقط ك Metadata وبصيغة redacted



تخضع Query و Export لسياسة الحساسية

Action safety: كتالوج العمليات قائم على البيانات؛ ولا يُدعى أي أمر عام على الأجهزة أو تغيير للإعدادات الحية.



بيانات شبكة منشؤها ومستوى الثقة بها واضحان.

صُمم 4SO Network لاتخاذ القرار بناءً على بيانات الشبكة؛ مع Confidence و Provenance كجزء من النموذج نفسه.

