

IP ANALYZER NEW FEATURES 2026

BY IDEO LAB

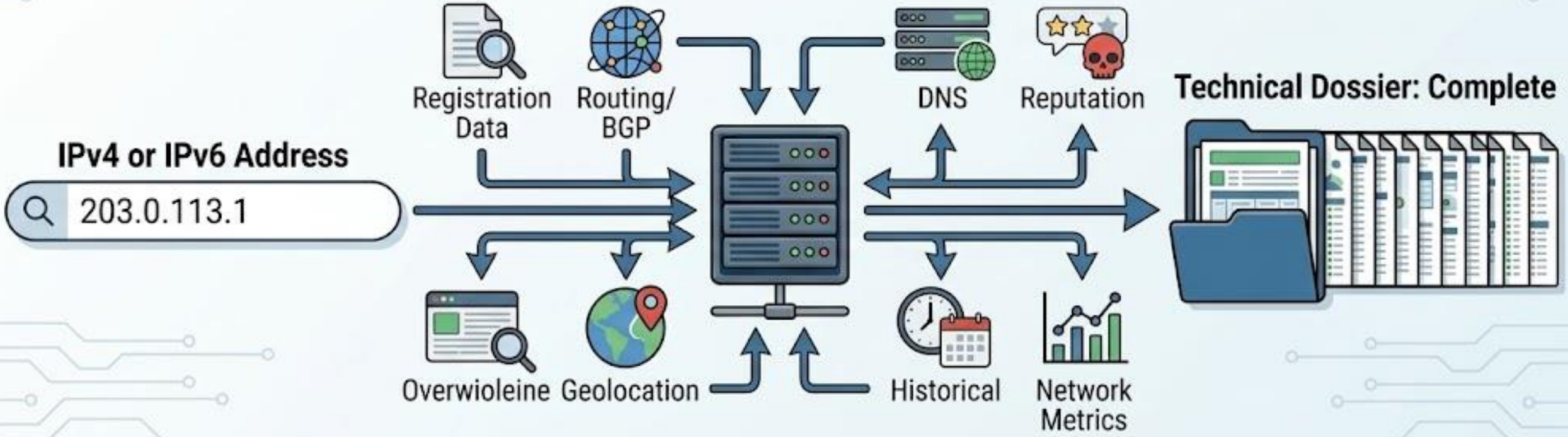
SEPTEMBER 19TH 2026

EARLY VERSION 0.9



IP ANALYZER

Building a Comprehensive Technical Profile



CAUTION



Attribution & Location of Network Infrastructure. No guarantee of Physical Address or Personal Identity (e.g., as per MaxMind)





SECURITY ANALYZER EXTENSION

IP ANALYZER

Couche de renseignement réseau, d’attribution technique et de qualification du risque

Une adresse IP n’est pas seulement un point d’entrée : c’est un indice technique, géographique, réseau et comportemental.



1. Introduction — transformer une IP en renseignement exploitable

Objectif : construire une capacité d’analyse profonde, structurée et réutilisable autour de toute adresse IP.

Constat

- Les informations IP sont dispersées entre registres, DNS, routage, géolocalisation, réputation et exposition de services.
- Une lecture isolée produit des conclusions fragiles, difficiles à comparer et rarement actionnables.
- IP Analyzer agrège ces signaux dans un modèle unique, explicable et relié au Security Analyzer.

Ambition

- Créer un couteau suisse d’analyse IP utilisable en standalone Linux et pilotable depuis le dashboard.
- Produire un rapport clair : origine probable, infrastructure, routes, signaux de risque et limites de confiance.
- Passer d’une donnée brute à une décision technique documentée.

2. Pourquoi — un besoin opérationnel récurrent

L’analyse IP devient une brique centrale pour comprendre l’exposition, les incidents, les anomalies et les dépendances réseau.

Qualification rapide

Identifier le propriétaire réseau, le pays, l’ASN, l’hébergeur et les indices de réputation.

Réduction du bruit

Distinguer une adresse banale, un proxy, un CDN, un relais, un hébergeur cloud ou une infrastructure suspecte.

Priorisation du risque

Classer les signaux selon leur impact potentiel et leur niveau de confiance.

Traçabilité

Conserver les résultats, horodatages, sources et chemins de raisonnement pour comparaison.

3. Périmètre fonctionnel — analyse profonde en couches

Chaque couche enrichit l'adresse IP avec un angle spécifique, puis alimente un moteur de corrélation.

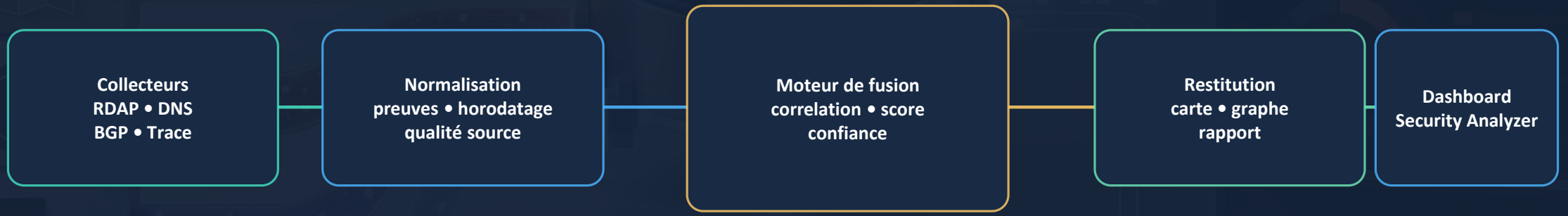
Identité réseau	WHOIS / RDAP, ASN, préfixe, organisation, contacts techniques
DNS & domaines	PTR, historique, domaines liés, cohérence des enregistrements
Routage	BGP, chemins, préfixes, anomalies, changements visibles
Géolocalisation	Pays, région, ville probable, cohérence multi-sources
Réputation	Listes de blocage, abus signalés, proxy/VPN/Tor, botnet connu
Exposition	Ports, bannières, TLS, technologies détectées, surface visible
Trace réseau	Traceroute, latence, hops, comparaison IPv4/IPv6 si disponible
Score explicable	Risque, confiance, preuves, limites et recommandations

4. Technologies — collecte, enrichissement, fusion, restitution

Une architecture modulaire permet d'ajouter des analyseurs sans rompre le cœur applicatif.

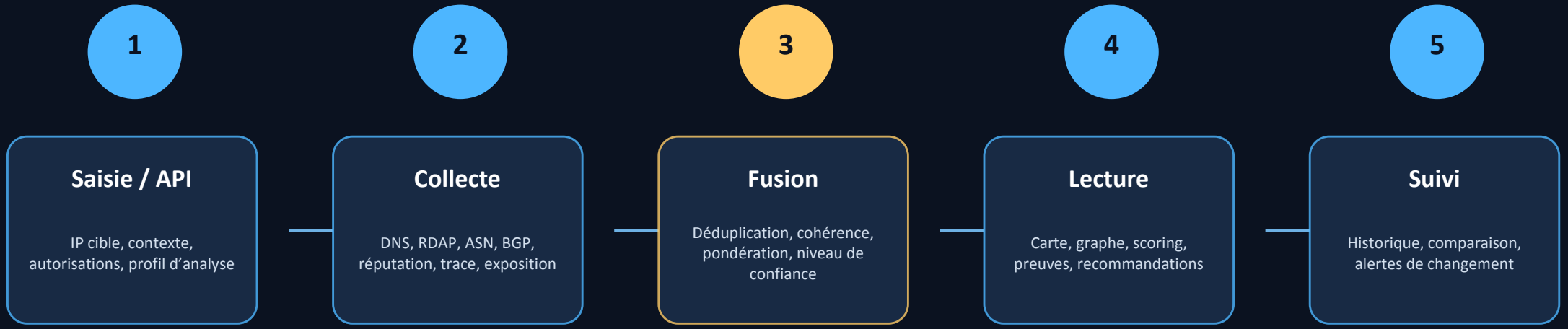
Principes techniques

- Python standalone, sans dépendance serveur externe obligatoire.
- Analyseurs indépendants, orchestrés en pipeline contrôlé.
- Résultats persistés, comparables et exportables.



5. Comment — déroulé d'une analyse IP

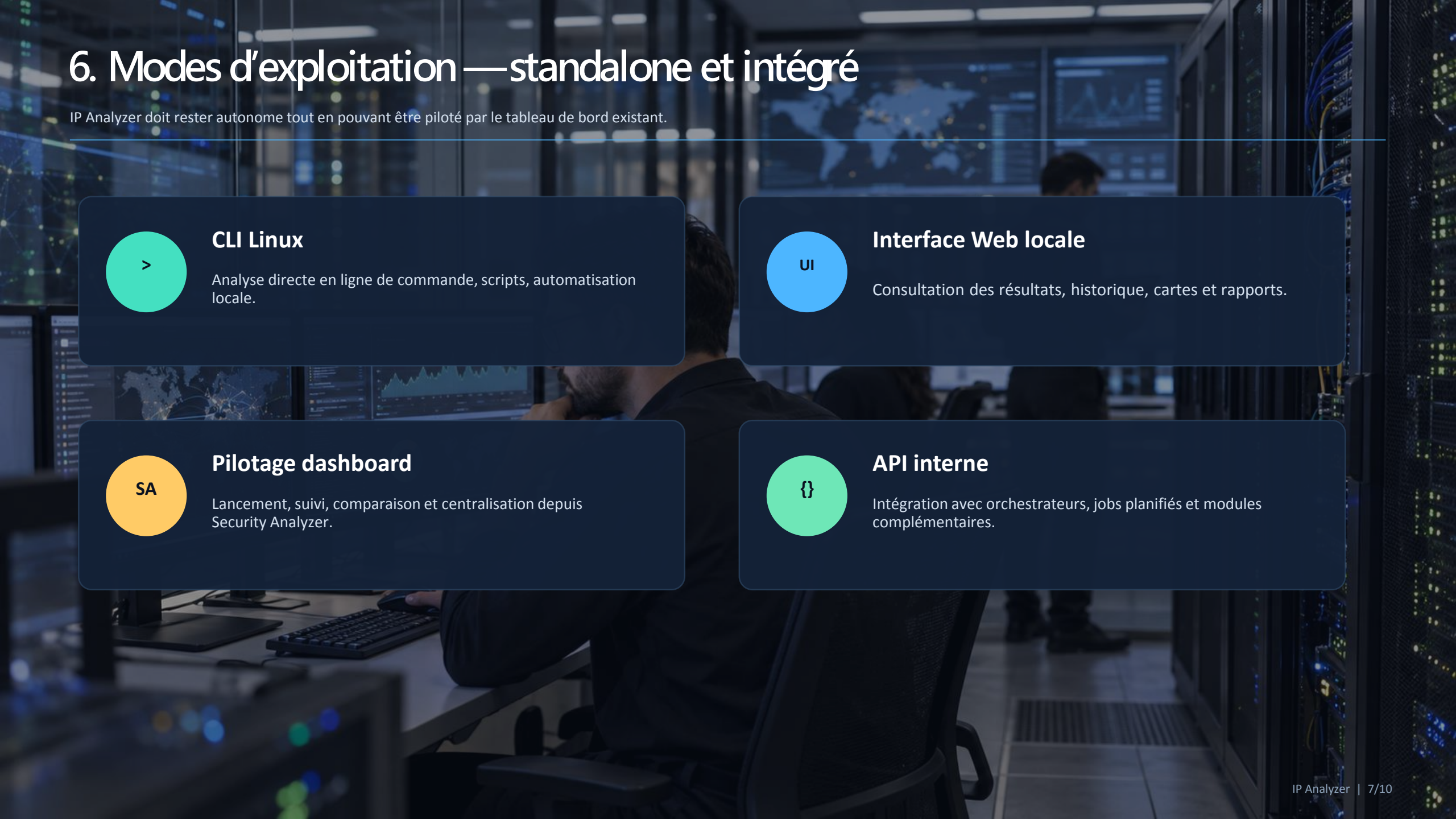
Le moteur collecte plusieurs familles de signaux, les compare, puis produit une synthèse argumentée.



Résultat attendu : une fiche IP complète, lisible, horodatée et expliquée, avec un score de risque séparé du score de confiance.

6. Modes d'exploitation — standalone et intégré

IP Analyzer doit rester autonome tout en pouvant être piloté par le tableau de bord existant.



CLI Linux

Analyse directe en ligne de commande, scripts, automatisation locale.

Interface Web locale

Consultation des résultats, historique, cartes et rapports.

Pilotage dashboard

Lancement, suivi, comparaison et centralisation depuis Security Analyzer.

API interne

Intégration avec orchestrateurs, jobs planifiés et modules complémentaires.

7. Gains & ROI — valeur mesurable sans promesse artificielle

La valeur vient de la réduction du temps d'analyse, de la cohérence des décisions et de la réutilisation de la plateforme existante.

Temps

moins de recherches manuelles dispersées

Risque

priorisation fondée sur preuves et confiance

Cohérence

même lecture entre opérateurs et rapports

Traçabilité

réemploi technique, historique et export

Lecture ROI

- Moins d'outils séparés à manipuler pour une même investigation.
- Rapports plus rapides à produire et plus simples à relire.
- Capitalisation des analyses précédentes par historique et comparaison.

Équation de valeur

ROI = temps économisé + réduction du risque d'erreur + meilleure priorisation + réutilisation technique

8. Gouvernance — sécurité, conformité et limites d'interprétation

Une analyse IP sérieuse doit distinguer preuve technique, probabilité et hypothèse.

Cadre d'usage

- Analyses autorisées
- Journalisation des actions
- Séparation observation / action

Qualité des preuves

- Score de confiance par source
- Contradictions visibles
- Horodatage systématique

Limites assumées

- Géolocalisation probabiliste
- CDN / VPN / proxy possibles
- Attribution humaine non garantie

9. Feuille de route — construction progressive et maîtrisée

Déployer par lots cohérents : fondation technique, enrichissement, visualisation, puis exploitation avancée.



Validation IP, RDAP/WHOIS, DNS, ASN, modèle de résultat.

Traceroute, BGP, préfixes, cohérence multi-sources.

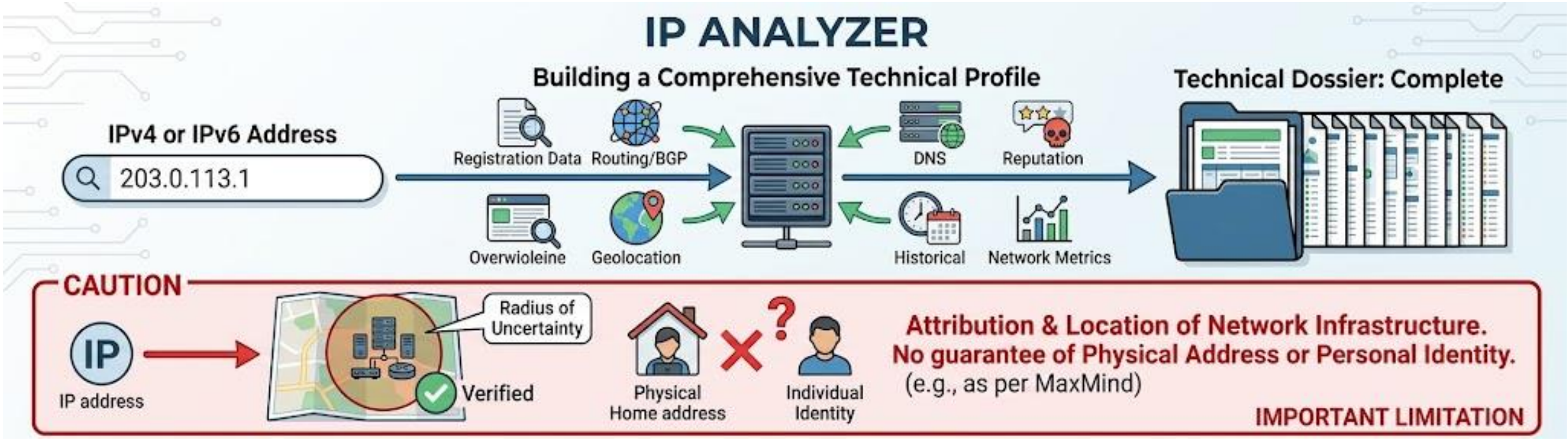
Réputation, scoring, confiance, justification des preuves.

Rapport, carte, graphe, historique, export.

Raccordement dashboard, API interne, orchestration.

Principe directeur : chaque lot doit ajouter une valeur visible, testable et documentée, sans rompre les fonctions existantes.

IP ANALYZER V 1.0





Je le concevrais comme un **IP Intelligence & Attribution Analyzer** : on lui donne **une IPv4 ou une IPv6**, et il construit progressivement un dossier technique complet en croisant renseignements d'enregistrement, routage Internet, géolocalisation, DNS, BGP, réputation, observations historiques et mesures réseau.

La limite fondamentale doit cependant être clairement affichée : **on peut attribuer et localiser une infrastructure réseau, mais pas garantir l'adresse physique ou l'identité de la personne utilisant l'IP.** MaxMind indique explicitement qu'une IP ne permet pas de localiser précisément un foyer ou un individu, et fournit justement un rayon d'incertitude pour ses coordonnées. MaxMind +1

IP ATTRIBUTION VERDICT

> IP: 203.xxx.xxx.xxx
> Type: IPv4 Public
> Country: Spain — **Confidence 99%**
> Probable Region: Comunidad Valenciana — **Confidence 86%**
> Probable City: Valencia — **Confidence 58%**
> Geolocation radius: ±35 km
> RIR: RIPE NCC
> Prefix: 203.xxx.xxx.0/24
> ASN: ASxxxxx
> Origin ASN: ASxxxxx
> Network Owner: Example Telecom España
> Operational Provider: Example Hosting SL
> Network Type: Datacenter / Hosting
> Anycast: No
> VPN: Unlikely
> Proxy: No evidence
> Tor Exit: No
> Residential Proxy: No evidence
> Reverse DNS: server14.example.net
> BGP RPKI: VALID
> Internet exposure: 443 / 80 / 22
> Known historical services: ...
> Reputation: LOW / MEDIUM / HIGH
> Last observed malicious activity: ...
> Infrastructure attribution confidence: **92 / 100**

IP ANALYZER AGENDA

- 1. IP Registry & Ownership Engine
- 2. ASN / BGP Deep Analyzer
- 3. RPKI / Routing Security
- 4. Multi-Source Geolocation Engine
- 5. Network-Type Classification
- 6. Reverse DNS Intelligence
- 7. DNS / Domain Association Engine
- 8. TLS Certificate Intelligence
- 9. Internet Exposure Intelligence
- 10. Reputation & Threat Intelligence

IP ANALYZER AGENDA – PART 2

- 11. Le véritable traceroute
- 12. Mais un seul traceroute ne suffit surtout pas
- 13. Latency-Based Geolocation
- 14. Scamper serait également très intéressant
- 15. Historical IP Intelligence
- 16. Le moteur de corrélation serait le cœur du produit
- 17. Et surtout : un Confidence Engine
- 18. Dashboard que je vois pour Security Analyzer

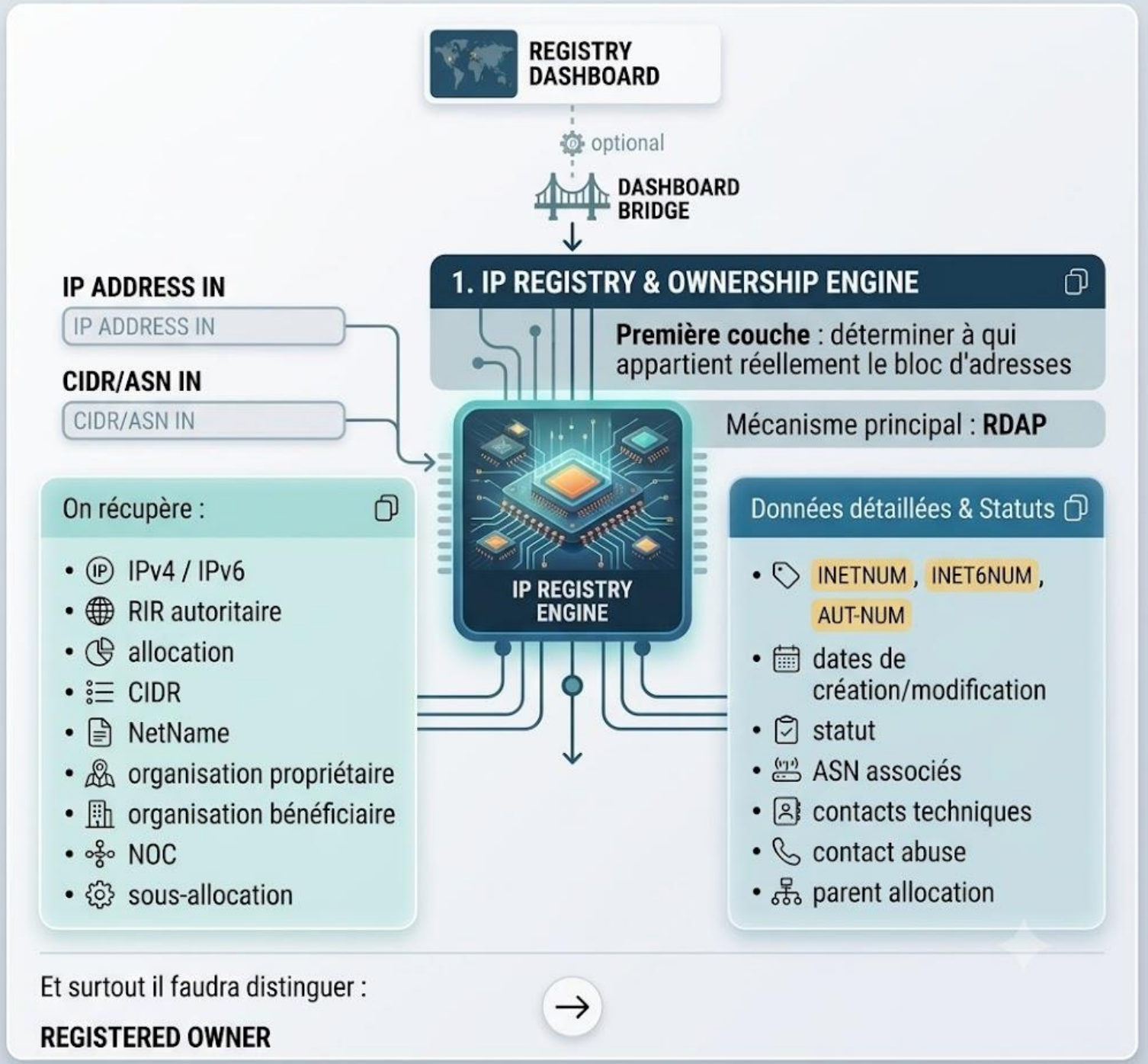
1. IP Registry & Ownership Engine

Première couche : déterminer **à qui appartient réellement le bloc d'adresses**.

Je privilégierais désormais **RDAP**, pas le vieux WHOIS comme mécanisme principal. RDAP permet notamment d'interroger les RIR et retourne des structures JSON directement exploitables. ARIN permet explicitement des recherches IP/CIDR/ASN avec RDAP, et RIPE fournit également RDAP pour ses objets `INETNUM`, `INET6NUM` et `AUT-NUM`. host-252-47.arin... +1

On récupère :

- IPv4 / IPv6
- RIR autoritaire
- allocation
- CIDR
- plage IP
- NetName
- organisation propriétaire
- organisation bénéficiaire
- dates de création
- dates de modification
- statut
- ASN associés
- NOC
- contacts techniques
- contact abuse
- parent allocation
- sous-allocation éventuelle.


REGISTRY DASHBOARD
optional
DASHBOARD BRIDGE
1. IP REGISTRY & OWNERSHIP ENGINE
Première couche : déterminer à qui appartient réellement le bloc d'adresses
IP ADDRESS IN
IP ADDRESS IN
CIDR/ASN IN
CIDR/ASN IN
Mécanisme principal : RDAP
IP REGISTRY ENGINE
On récupère :
IPv4 / IPv6
RIR autoritaire
allocation
CIDR
NetName
organisation propriétaire
organisation bénéficiaire
NOC
sous-allocation
Données détaillées & Statuts
INETNUM , INET6NUM , AUT-NUM
dates de création/modification
statut
ASN associés
contacts techniques
contact abuse
parent allocation
Et surtout il faudra distinguer :
REGISTERED OWNER

2. ASN / BGP Deep Analyzer

Là, cela commence à devenir beaucoup plus puissant.

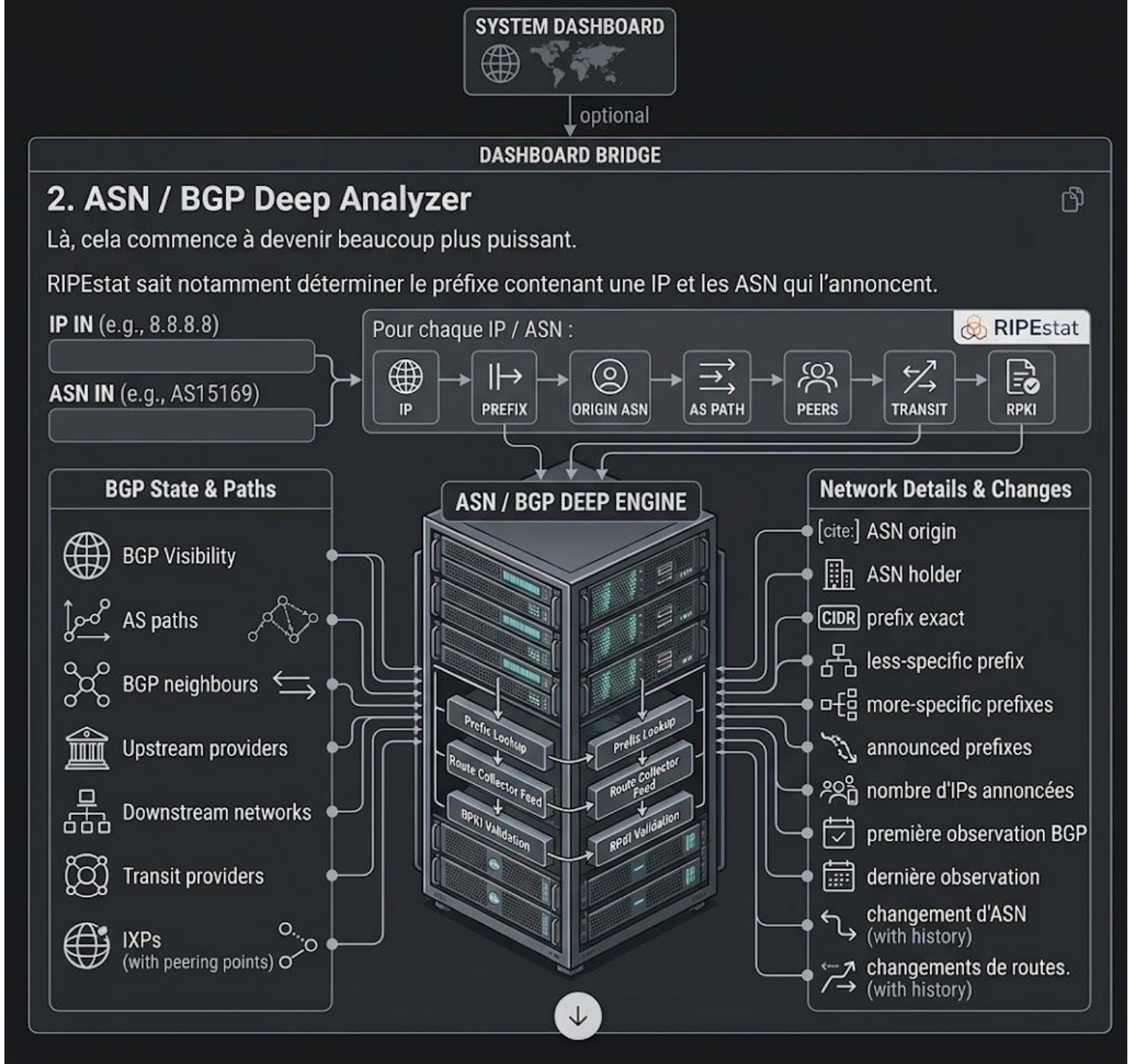
Pour chaque IP :

```
IP → PREFIX → ORIGIN ASN → AS PATH → PEERS → TRANSIT → RPKI
```

RIPEstat sait notamment déterminer le préfixe contenant une IP et les ASN qui l'annoncent. stat.ripe.net

Je veux afficher :

- ASN origin
- ASN holder
- prefix exact
- less-specific prefix
- more-specific prefixes
- BGP visibility
- AS paths
- BGP neighbours
- upstream providers
- downstream networks
- transit providers
- IXPs
- announced prefixes
- nombre d'IPs annoncées
- première observation BGP
- dernière observation
- changement d'ASN


SYSTEM DASHBOARD
optional
DASHBOARD BRIDGE
2. ASN / BGP Deep Analyzer
Là, cela commence à devenir beaucoup plus puissant.
RIPEstat sait notamment déterminer le préfixe contenant une IP et les ASN qui l'annoncent.
IP IN (e.g., 8.8.8.8)
ASN IN (e.g., AS15169)
Pour chaque IP / ASN :
RIPEstat
IP
PREFIX
ORIGIN ASN
AS PATH
PEERS
TRANSIT
RPKI
BGP State & Paths
BGP Visibility
AS paths
BGP neighbours
Upstream providers
Downstream networks
Transit providers
IXPs
(with peering points)
ASN / BGP DEEP ENGINE
Prefix Lookup
Route Collector Feed
RPKI Validation
Network Details & Changes
ASN origin
ASN holder
prefix exact
less-specific prefix
more-specific prefixes
announced prefixes
nombre d'IPs annoncées
première observation BGP
dernière observation
changement d'ASN
(with history)
changements de routes.
(with history)

RIPE conserve même un historique des annonces et de leurs ASN d'origine. stat-ui.stat.ripe.net

Il existe aussi les BGP Updates :

- Announcement
- Withdrawal
- timestamp
- AS path
- collector
- prefix.

stat.ripe.net

On pourrait donc avoir une timeline :

BGP HISTORY

```
2024 ———————— 2025 ———————— 2026
```

avec changement d'opérateur, annonces, retraits ou apparition de nouveaux prefixes.

3. RPKI / Routing Security

Très intéressant pour notre Security Analyzer.

On vérifie :

RPKI VALID

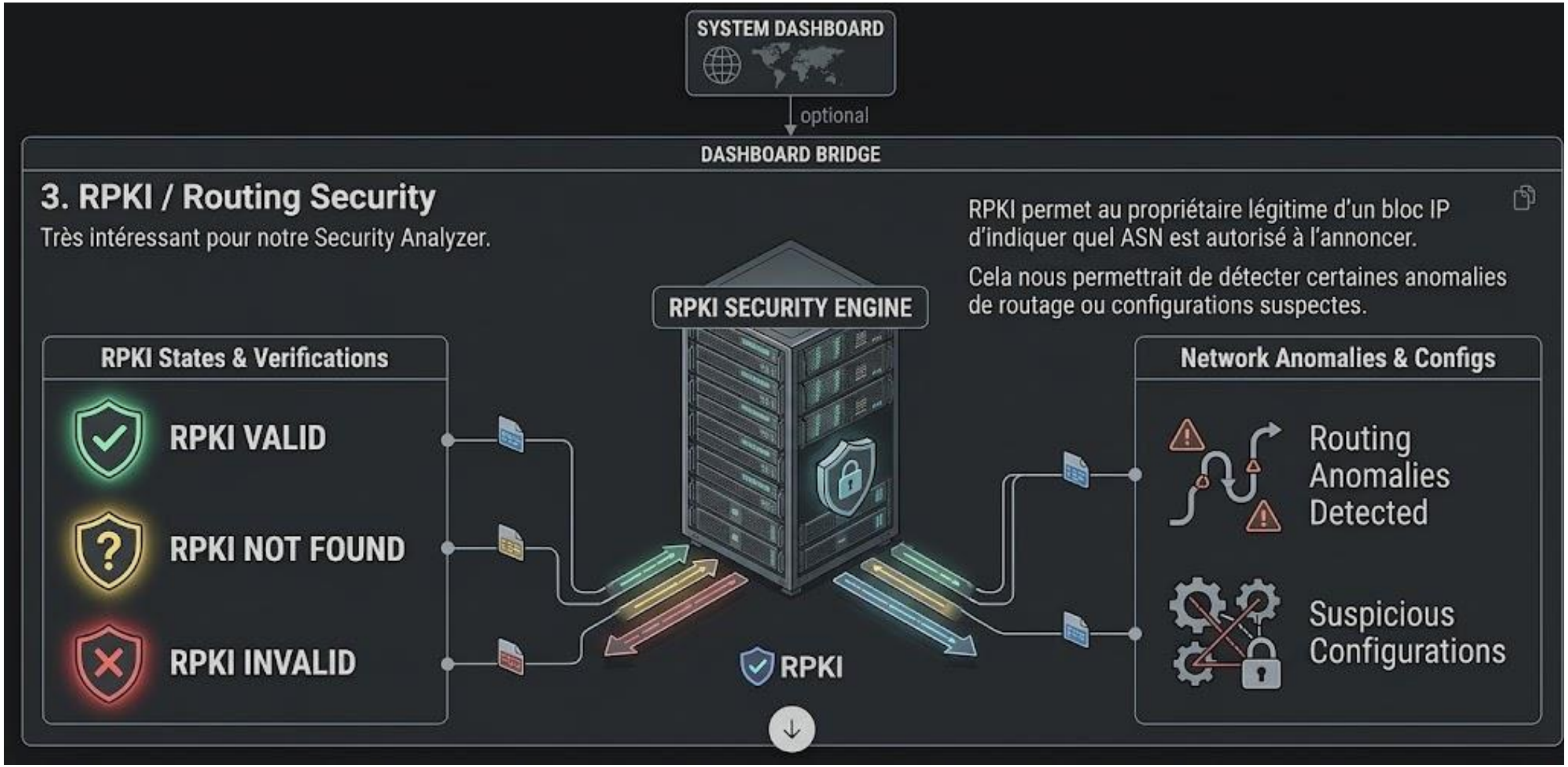
RPKI NOT FOUND

RPKI INVALID

RPKI permet au propriétaire légitime d'un bloc IP d'indiquer quel ASN est autorisé à l'annoncer.

rpki.readthedocs.io +1

Cela nous permettrait de détecter certaines anomalies de routage ou configurations suspectes.


SYSTEM DASHBOARD
optional
DASHBOARD BRIDGE
3. RPKI / Routing Security
Très intéressant pour notre Security Analyzer.
RPKI permet au propriétaire légitime d'un bloc IP d'indiquer quel ASN est autorisé à l'annoncer.
Cela nous permettrait de détecter certaines anomalies de routage ou configurations suspectes.
RPKI SECURITY ENGINE
RPKI States & Verifications
RPKI VALID
RPKI NOT FOUND
RPKI INVALID
Network Anomalies & Configs
Routing Anomalies Detected
Suspicious Configurations
RPKI

4. Multi-Source Geolocation Engine

Surtout, **pas une seule base.**

Je croiserais par exemple :

- MaxMind
- IPinfo
- DB-IP
- IP2Location
- données RIR
- BGP
- reverse DNS
- informations opérateur
- données traceroute.

Le moteur pourrait calculer :

GEO CONSENSUS

Source	Country	City	Radius
MaxMind	Spain	Valencia	50 km
IPinfo	Spain	Valencia	—
DB-IP	Spain	Valencia	—
Reverse DNS	Spain	VLC	—
RTT inference	East Spain	–	100 km

Puis :

Geolocation consensus: Valencia region

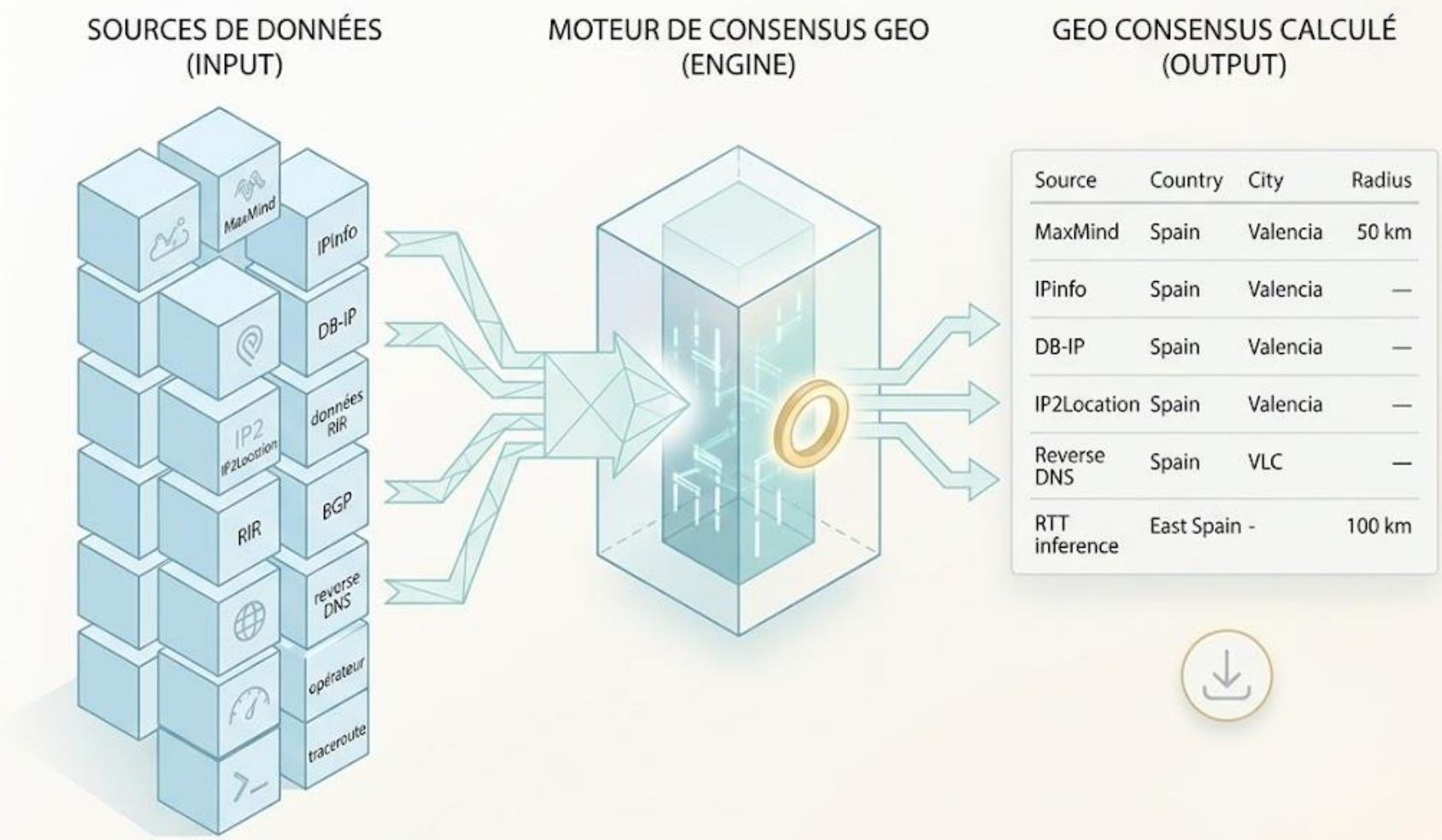
Confidence: 81%

Et non afficher bêtement une latitude/longitude comme si nous connaissions l'immeuble.

MaxMind fournit justement un `accuracy_radius` autour de ses coordonnées et indique une confiance d'environ 67 % pour que la localisation réelle se trouve dans ce cercle. MaxMind +1

4. Multi-Source Geolocation Engine

Surtout, pas une seule base.



Source	Country	City	Radius
MaxMind	Spain	Valencia	50 km
IPinfo	Spain	Valencia	—
DB-IP	Spain	Valencia	—
IP2Location	Spain	Valencia	—
Reverse DNS	Spain	VLC	—
RTT inference	East Spain	-	100 km

5. Network-Type Classification

Très important.

Il faudra déterminer si l'IP est :

- Residential ISP
- Business ISP
- Mobile
- Hosting
- VPS
- Dedicated server
- Cloud
- CDN
- VPN
- Proxy
- Residential proxy
- Tor exit
- Search engine crawler
- Security scanner
- Bot infrastructure
- University
- Government
- Satellite network
- Anycast.

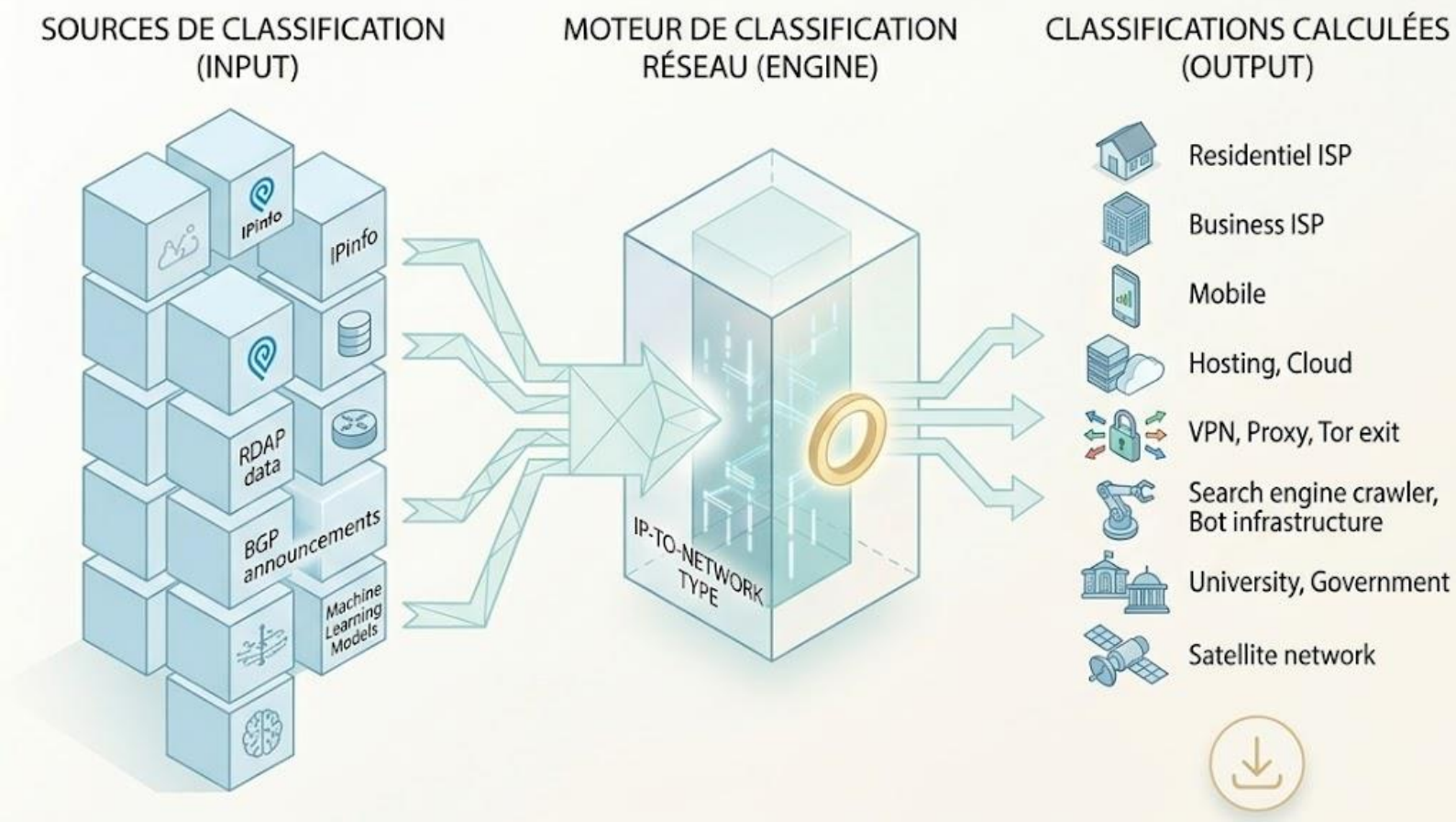
IPinfo fournit notamment de la détection VPN, proxy, Tor et hosting. support.ipinfo.io

Cette classification change complètement l'interpréta[illegible] de la localisation.

5. Network-Type Classification

Très important.

Il faudra déterminer si l'IP est :



IPinfo fournit notamment de la détection VPN, proxy, Tor et hosting. support.ipinfo.io

Cette classification change complètement l'interprétation de la localisation.

6. Reverse DNS Intelligence

On effectue :

`IP → PTR`

puis :

`PTR → A / AAAA`

et on vérifie la cohérence.

Exemple :

`185.x.x.x`

→ `srv42.paris.examplehosting.com`

Le hostname peut révéler :

- opérateur
- pays
- ville
- datacenter
- router
- POP
- rôle du serveur.

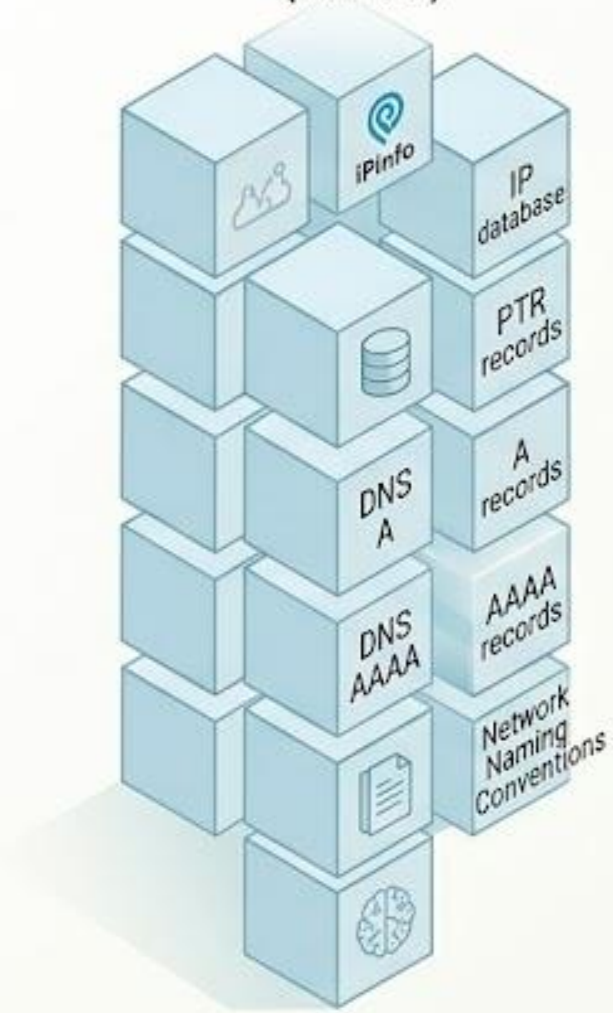
Certaines conventions de nommage réseau contiennent même des codes du genre :

`fra`

`ams`

6. Reverse DNS Intelligence

SOURCES DE DONNÉES (INPUT)



MOTEUR DE RECHERCHE INVERSE (ENGINE)



RÉSULTATS DE L'INTELLIGENCE (OUTPUT)



`185.x.x.x` → `srv42.paris.examplehosting.com`

`fra`

`ams`



Certaines conventions de nommage réseau contiennent même des codes du genre :

`fra`

`ams`

`lon`

`mad`

`cdg`

`iad`

`nyc`

`sin`

qui donnent des indices sur le Point of Presence.

Ils doivent naturellement être considérés comme **indices**, pas comme preuves absolues.

7. DNS / Domain Association Engine

On recherche ensuite les domaines associés historiquement ou actuellement à l'IP.

Avec :

- PTR
- DNS actuel
- Passive DNS
- certificats TLS
- Subject Alternative Names
- Certificate Transparency.

Cela permettra d'obtenir :

Associated Domains

`domain-a.com`

`api.domain-a.com`

`vpn.domain-b.net`

`old-domain-c.org`

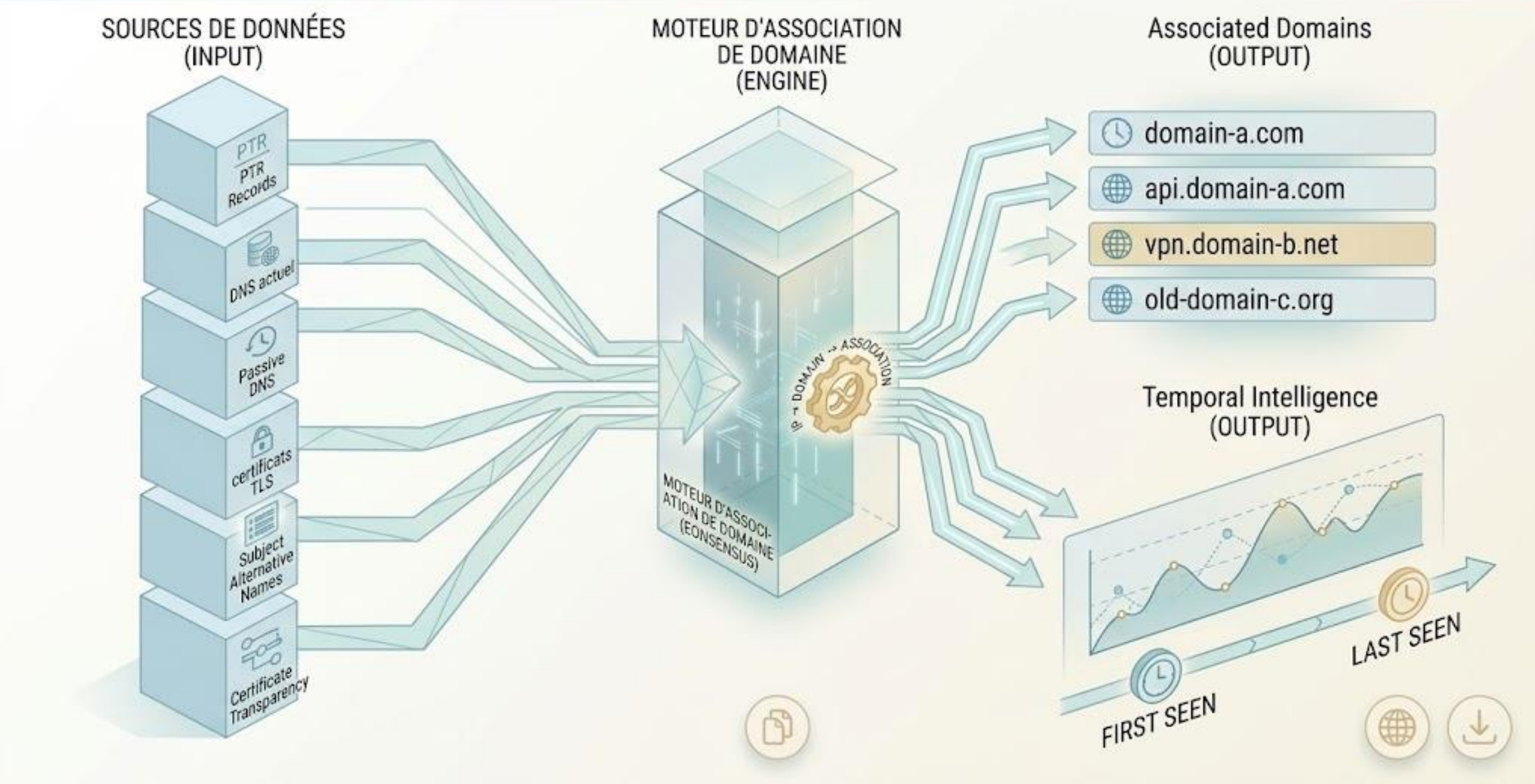
Puis :

FIRST SEEN

LAST SEEN

C'est extrêmement intéressant dans une investigation.

7. DNS / Domain Association Engine



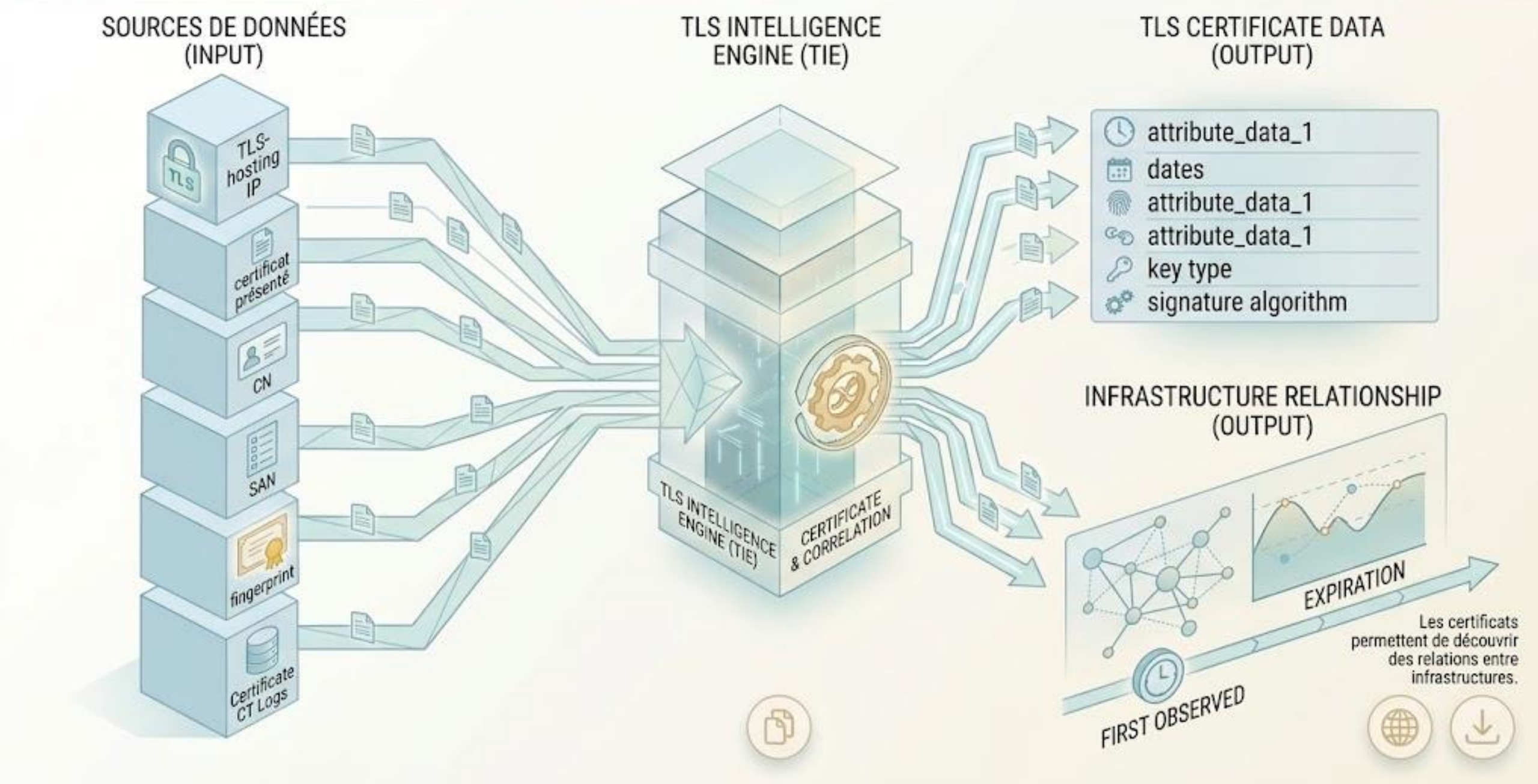
8. TLS Certificate Intelligence

Pour les IP hébergeant TLS :

- certificat présenté
- issuer
- CN
- SAN
- dates
- fingerprint
- serial
- key type
- signature algorithm
- expiration
- domains associés.

Les certificats peuvent permettre de découvrir des relations entre infrastructures qui ne sont pas évidentes au départ.

8. TLS Certificate Intelligence



9. Internet Exposure Intelligence

Ici je mettrais **Censys + Shodan** comme enrichissements facultatifs majeurs.

Shodan permet de récupérer les services précédemment observés sur une IP et dispose notamment d'un endpoint `host/{ip}`. Shodan Developer

Censys dispose maintenant de son API Platform v3 pour récupérer directement un host donné, avec services, réseau, certificats et autres observations. Censys Documen... +1

On pourrait montrer :

Observed Internet Services

```
22/tcp SSH OpenSSH ...
```

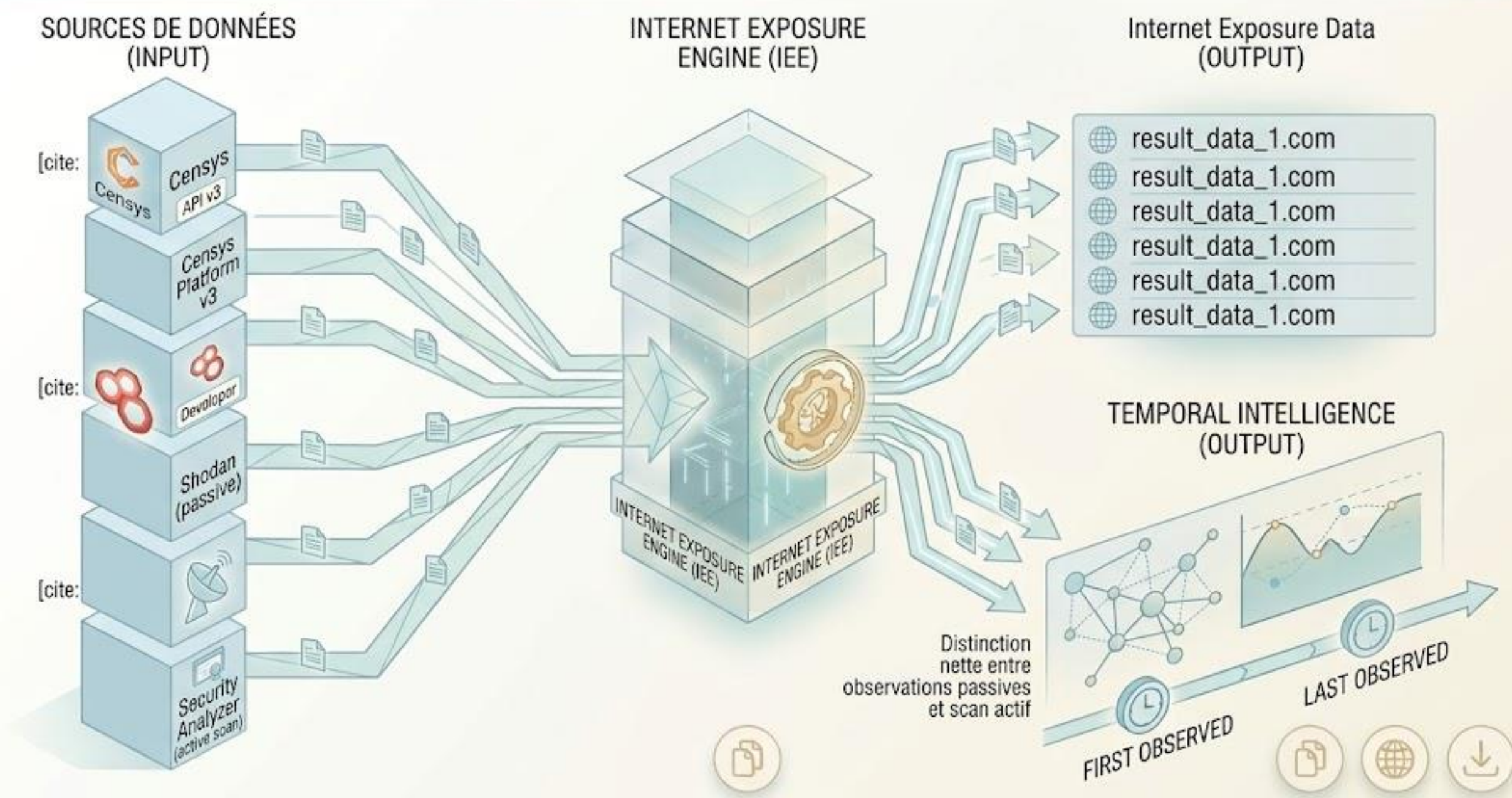
```
443/tcp HTTPS nginx ...
```

```
8443/tcp HTTPS ...
```

etc.

Mais ici je ferais une distinction très nette entre **observations passives provenant de bases Internet** et **scan actif**, ce dernier n'étant exécuté que dans le cadre autorisé du Security Analyzer.

9. Internet Exposure Intelligence



10. Reputation & Threat Intelligence

Ensuite une section :

IP REPUTATION

On interroge notamment :

- VirusTotal
- GreyNoise
- AbuseIPDB
- éventuellement Spamhaus selon licence/API
- données internes du Security Analyzer.

VirusTotal fournit pour une IP des informations comme ASN, propriétaire AS, pays et résultats d'analyses.

VirusTotal

GreyNoise peut fournir :

- owner
- ASN
- PTR
- country
- actors
- tags
- activité de scan
- classification.

GreyNoise

AbuseIPDB expose les signalements associés à une IP et permet aussi d'interroger un bloc CIDR. AbuseIPDB

AbuseIPDB expose les signalements associés à une IP et permet aussi d'interroger un bloc CIDR. AbuseIPDB

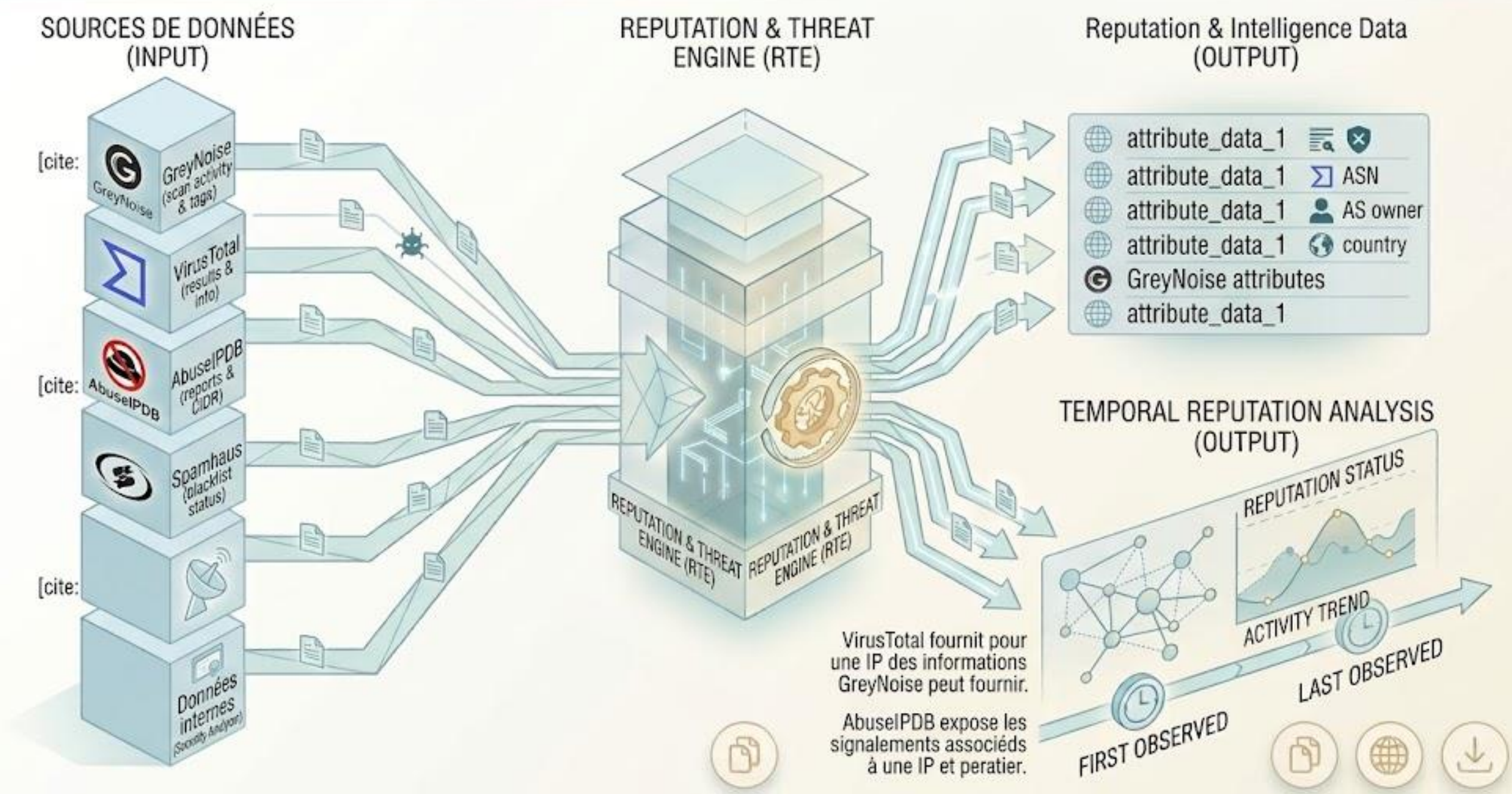
On pourrait créer :

THREAT SCORE

```
0 ———————————— 100
```

avec explication de chaque contribution au score.

10. Reputation & Threat Intelligence



11. Le véritable traceroute

Et là je veux quelque chose de beaucoup plus spectaculaire que la sortie texte traditionnelle.

On effectue plusieurs méthodes :

ICMP traceroute

UDP traceroute

TCP traceroute

et idéalement variante **Paris Traceroute** pour mieux gérer certains chemins avec load-balancing.

RIPE Atlas supporte justement les traceroutes UDP, ICMP et TCP ainsi que des options Paris traceroute.

RIPE Atlas

Chaque hop deviendrait :

`IP → ASN → Provider → Country → City/POP → RTT`

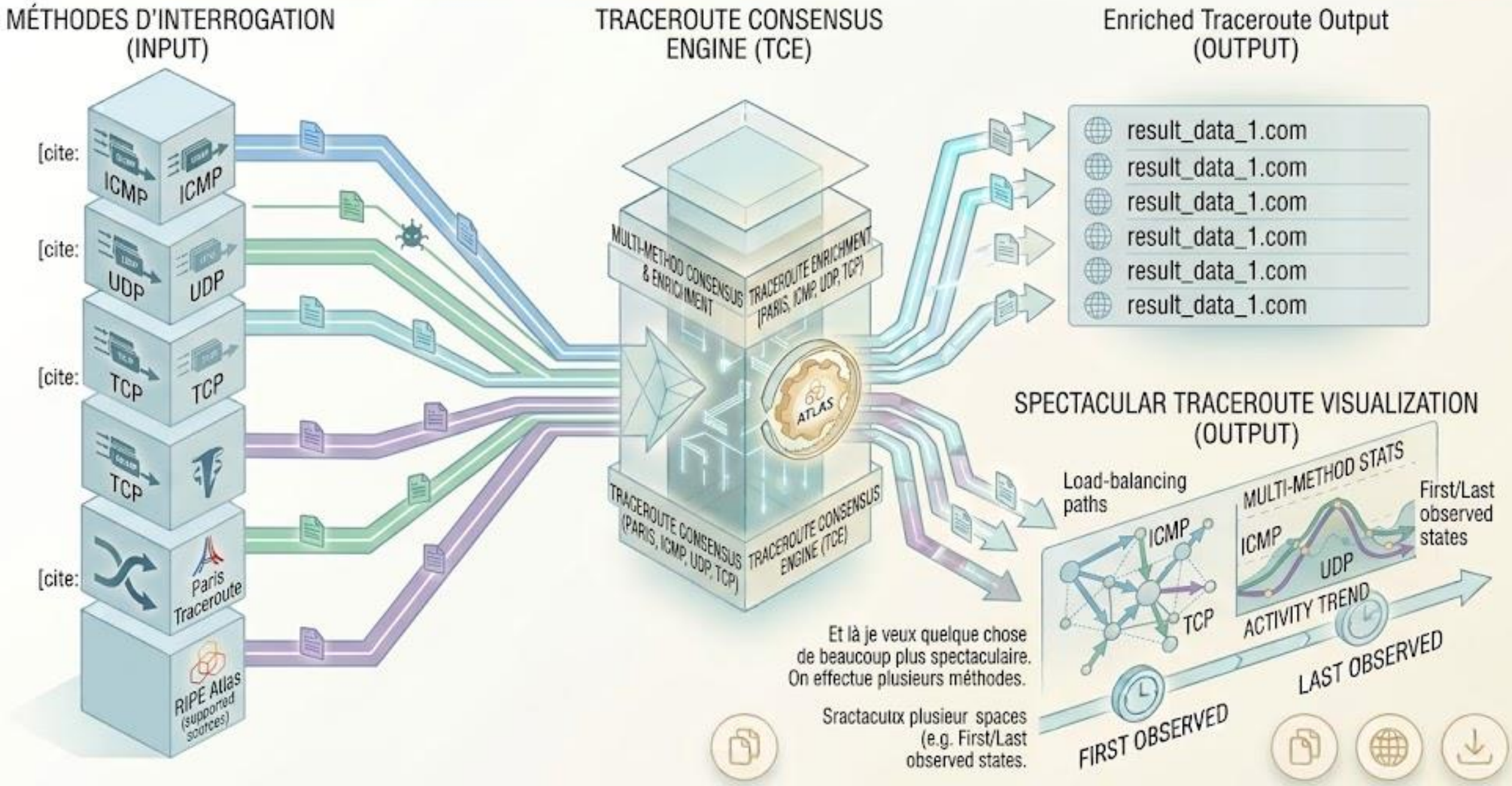
Par exemple :

```
ALICANTE
   |
   |  8 ms
   ▼
ISP ACCESS NETWORK
ASxxxx
   |
   |  15 ms
   ▼
MADRID
ASxxxx
```

```
ALICANTE
   |
   |  8 ms
   ▼
ISP ACCESS NETWORK
ASxxxx
   |
   |  15 ms
   ▼
MADRID
ASxxxx
   |
   |  31 ms
   ▼
PARIS
ASxxxx
   |
   |  43 ms
   ▼
AMSTERDAM
ASxxxxx
   |
   ▼
TARGET IP
```

Avec une vraie visualisation graphique dans le dashboard.

11. Le véritable traceroute



12. Mais un seul traceroute ne suffit surtout pas

C'est ici que notre produit peut devenir réellement supérieur à beaucoup de « IP lookup tools ».

Un traceroute depuis notre serveur espagnol ne donne qu'une vision :

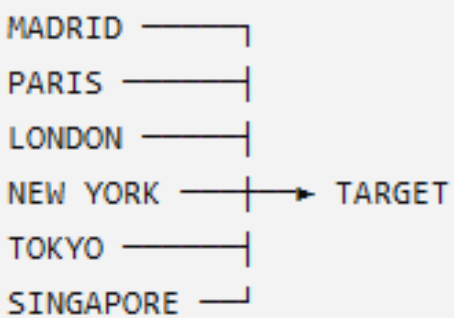
Spain → Target

Je voudrais effectuer des mesures depuis plusieurs endroits du monde :

- Spain
- France
- Germany
- UK
- USA East
- USA West
- Singapore
- Japan
- Australia.

RIPE Atlas permet précisément de lancer des mesures depuis des probes sélectionnées par pays, région, ASN, etc. RIPE Atlas +1

MULTI-VANTAGE IP TRACE

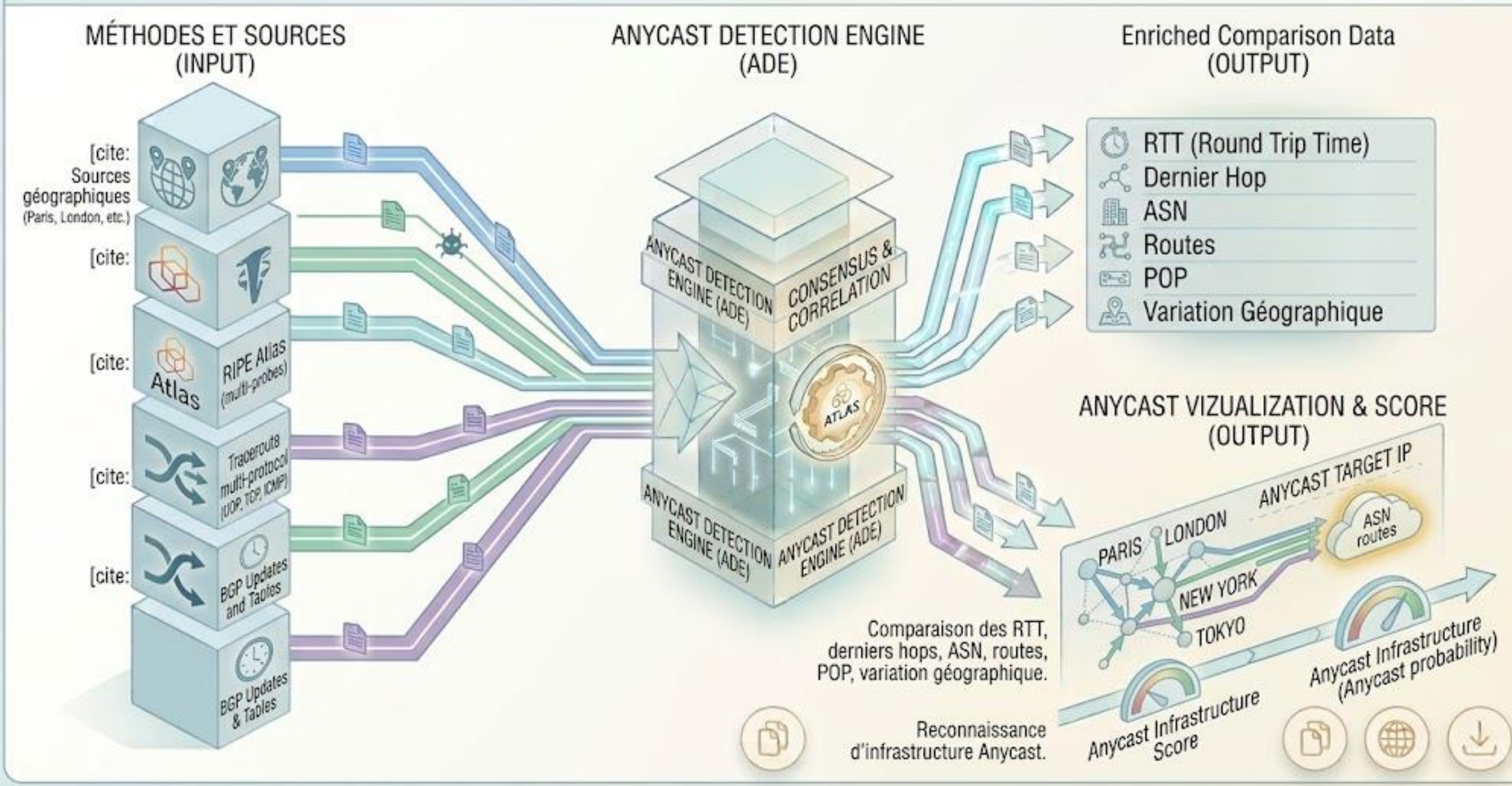


Et l'on compare :

- RTT
- dernier hop
- ASN
- routes
- POP
- variation géographique.

C'est extrêmement utile pour reconnaître notamment les infrastructures **Anycast**.

12. MULTI-VANTAGE IP TRACE (ANYCAST DETECTION)



13. Latency-Based Geolocation

On peut même ajouter notre propre moteur.

Si différents probes mesurent :

Madrid → IP : `11 ms`

Paris → IP : `31 ms`

London → IP : `38 ms`

New York → IP : `105 ms`

Singapore → IP : `210 ms`

on peut calculer des contraintes géographiques.

Cela ne donne pas une adresse.

Mais cela permet parfois de dire :

Les données GeoIP prétendent que l'IP est à New York, mais les mesures réseau sont incompatibles avec cette localisation.

Donc :

GEO CONSISTENCY

```
Database geolocation : Germany

Network latency evidence : Western Europe

Traceroute evidence : Frankfurt POP
```

LATENCY-BASED IP GEOLOCATION ANALYSIS

Correlating latency, topology, and geolocation evidence



GEO CONSISTENCY

MULTI-EVIDENCE CORRELATION

DATABASE GEOLOCATION

Database geolocation:

Germany

- High confidence match

NETWORK LATENCY EVIDENCE

Network latency evidence:

Western Europe

LATENCY DISTRIBUTION (TO IP NODE)



Closest cluster: Western Europe (0 – 40ms)

TRACEROUTE EVIDENCE

Traceroute evidence:

Frankfurt POP



Final hop in Frankfurt

ASXXX.X (POP)

EVIDENCE CONSISTENT

All signals align on Western Europe, Frankfurt as the most likely location.

ANALYSIS TIMESTAMP	TARGET IP	METHODOLOGY	CONFIDENCE SCORE	
2025-05-21 14:32:18 UTC	203.0.113.42	Latency Triangulation + Topology Mapping		HIGH 92/100

14. Scamper serait également très intéressant

Même si nous conservons notre philosophie standalone, il faut regarder ses techniques pour notre moteur interne.

CAIDA maintient toujours **Scamper en 2026** ; une version datée du **13 juillet 2026** est disponible. Il sait faire IPv4/IPv6, ping, traceroute, MDA traceroute, alias resolution, DNS, HTTP et plusieurs techniques avancées de topologie. CAIDA

Particulièrement intéressant :

alias resolution

Cela tente de déterminer si plusieurs interfaces IP appartiennent en réalité **au même routeur.**

Pour notre produit, nous pouvons soit intégrer Scamper comme moteur optionnel, soit nous inspirer de ses algorithmes pour notre moteur maison.

SCAMPER

ADVANCED NETWORK TOPOLOGY ENGINE

ENGINE v2.7.1
UPTIME: 47d 12h 33m 19s ● LIVE

ACTIVE CAPABILITIES

- **IPv4 / IPv6** — DUAL STACK DISCOVERY — ● ACTIVE
- **PING** — LATENCY & REACHABILITY — ● ACTIVE
- **TRACEROUTE** — PATH DISCOVERY — ● ACTIVE
- **MDA TRACEROUTE** — MULTIPATH DISCOVERY — ● ACTIVE
- **ALIAS RESOLUTION** — ROUTER IDENTIFICATION — ● ACTIVE
- **DNS** — RESOLUTION & REVERSE — ● ACTIVE
- **HTTP** — SERVICE DETECTION — ● ACTIVE
- **TOPOLOGY MAPPING** — GRAPH & VISUALIZATION — ● ACTIVE



ALIAS RESOLUTION

● MERGING INTO SINGLE ROUTER

IDENTIFIED INTERFACES (5)

192.168.1.1
198.51.100.10
203.0.113.15
172.16.0.1
10.0.0.1

↓

RESOLVED TO **203.0.113.1**

TOPOLOGY SUMMARY

ROUTERS (L3)	128
INTERFACES	512
LINKS	1,024
ALIASES RESOLVED	37

VIEW: 3D TOPOLOGY

LIVE METRICS

ACTIVE PROBES	1,248
PPS (OUT)	23.7K
DISCOVERY RATE	98.6%

DATA STREAM

MULTI-PROTOCOL DISCOVERY DATA FLOWING INTO SCAMPER ENGINE

PROTOCOL LAYER COVERAGE

L3 IP	ICMP	UDP	TCP	DNS	MD5 / IP-ID
IPv4 / IPv6	PING / ERROR	TRACEROUTE	HTTP / HTTPS	RESOLUTION	ALIAS SIGNALS

CAIDA
Cooperative Association for Internet Data Analysis
www.caida.org

15. Historical IP Intelligence

C'est une fonction que je considère indispensable.

Une IP aujourd'hui n'est qu'une photographie.

Nous devons afficher :

2022

2023

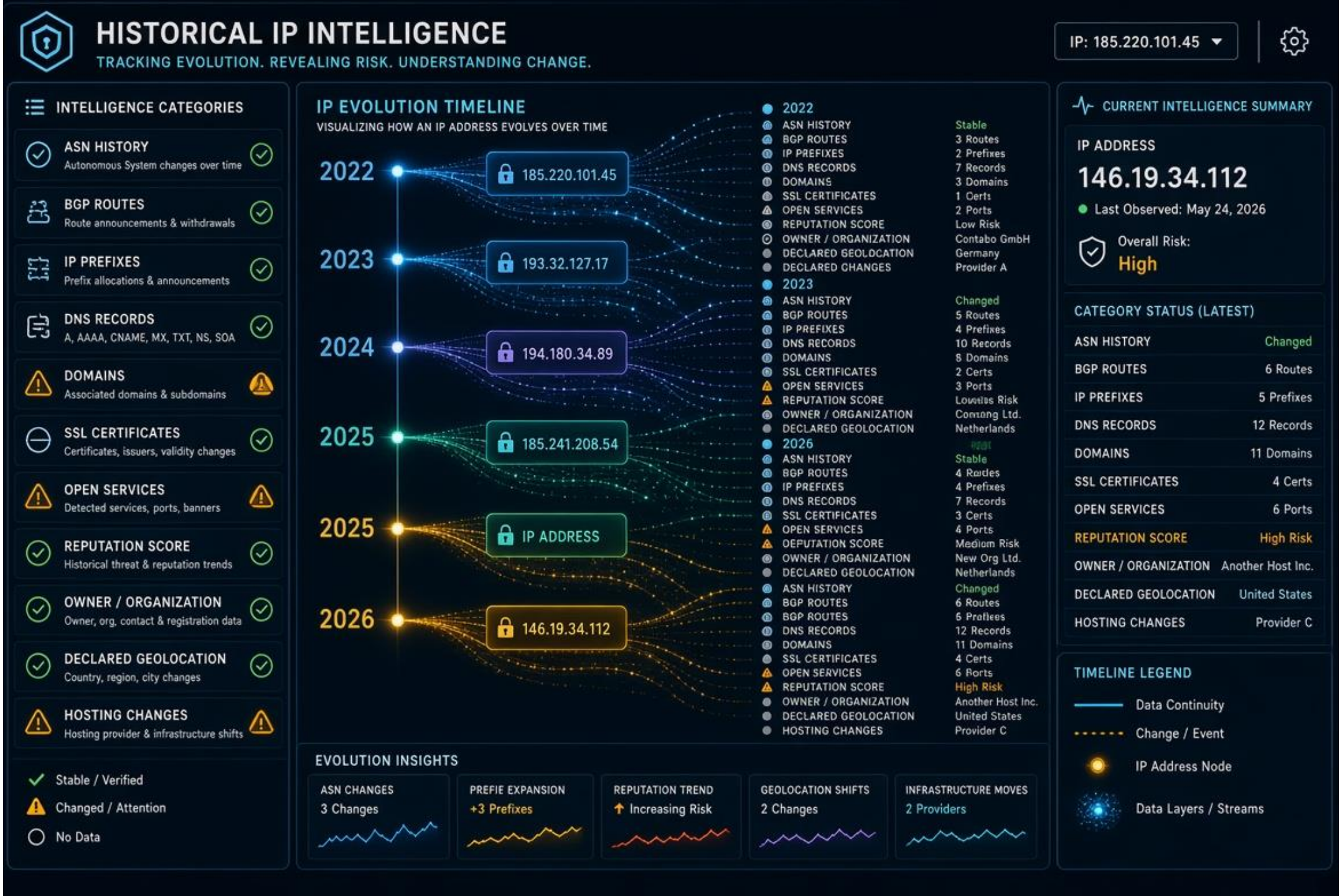
2024

2025

2026

avec :

- ASN historique
- routes BGP
- prefixes
- DNS
- domaines
- certificats
- services
- reputation
- propriétaire
- localisation déclarée
- changements d'hébergement.


HISTORICAL IP INTELLIGENCE
TRACKING EVOLUTION. REVEALING RISK. UNDERSTANDING CHANGE.
IP: 185.220.101.45
INTELLIGENCE CATEGORIES
ASN HISTORY
Autonomous System changes over time
BGP ROUTES
Route announcements & withdrawals
IP PREFIXES
Prefix allocations & announcements
DNS RECORDS
A, AAAA, CNAME, MX, TXT, NS, SOA
DOMAINS
Associated domains & subdomains
SSL CERTIFICATES
Certificates, issuers, validity changes
OPEN SERVICES
Detected services, ports, banners
REPUTATION SCORE
Historical threat & reputation trends
OWNER / ORGANIZATION
Owner, org, contact & registration data
DECLARED GEOLOCATION
Country, region, city changes
HOSTING CHANGES
Hosting provider & infrastructure shifts
Stable / Verified
Changed / Attention
No Data
IP EVOLUTION TIMELINE
VISUALIZING HOW AN IP ADDRESS EVOLVES OVER TIME
2022
185.220.101.45
2023
193.32.127.17
2024
194.180.34.89
2025
185.241.208.54
2025
IP ADDRESS
2026
146.19.34.112
2022
ASN HISTORY Stable
BGP ROUTES 3 Routes
IP PREFIXES 2 Prefixes
DNS RECORDS 7 Records
DOMAINS 3 Domains
SSL CERTIFICATES 1 Certs
OPEN SERVICES 2 Ports
REPUTATION SCORE Low Risk
OWNER / ORGANIZATION Contabo GmbH
DECLARED GEOLOCATION Germany
DECLARED CHANGES Provider A
2023
ASN HISTORY Changed
BGP ROUTES 5 Routes
IP PREFIXES 4 Prefixes
DNS RECORDS 10 Records
DOMAINS 8 Domains
SSL CERTIFICATES 2 Certs
OPEN SERVICES 3 Ports
REPUTATION SCORE Low Risk
OWNER / ORGANIZATION Contabo Ltd.
DECLARED GEOLOCATION Netherlands
2026
ASN HISTORY Stable
BGP ROUTES 4 Routes
IP PREFIXES 4 Prefixes
DNS RECORDS 7 Records
SSL CERTIFICATES 3 Certs
OPEN SERVICES 4 Ports
REPUTATION SCORE Medium Risk
OWNER / ORGANIZATION New Org Ltd.
DECLARED GEOLOCATION Netherlands
ASN HISTORY Changed
BGP ROUTES 6 Routes
BGP ROUTES 5 Prefixes
DNS RECORDS 12 Records
DOMAINS 11 Domains
SSL CERTIFICATES 4 Certs
OPEN SERVICES 6 Ports
REPUTATION SCORE High Risk
OWNER / ORGANIZATION Another Host Inc.
DECLARED GEOLOCATION United States
HOSTING CHANGES Provider C
EVOLUTION INSIGHTS
ASN CHANGES
3 Changes
PREFIE EXPANSION
+3 Prefixes
REPUTATION TREND
Increasing Risk
GEOLOCATION SHIFTS
2 Changes
INFRASTRUCTURE MOVES
2 Providers
CURRENT INTELLIGENCE SUMMARY
IP ADDRESS
146.19.34.112
Last Observed: May 24, 2026
Overall Risk:
High
CATEGORY STATUS (LATEST)
ASN HISTORY Changed
BGP ROUTES 6 Routes
IP PREFIXES 5 Prefixes
DNS RECORDS 12 Records
DOMAINS 11 Domains
SSL CERTIFICATES 4 Certs
OPEN SERVICES 6 Ports
REPUTATION SCORE High Risk
OWNER / ORGANIZATION Another Host Inc.
DECLARED GEOLOCATION United States
HOSTING CHANGES Provider C
TIMELINE LEGEND
Data Continuity
Change / Event
IP Address Node
Data Layers / Streams

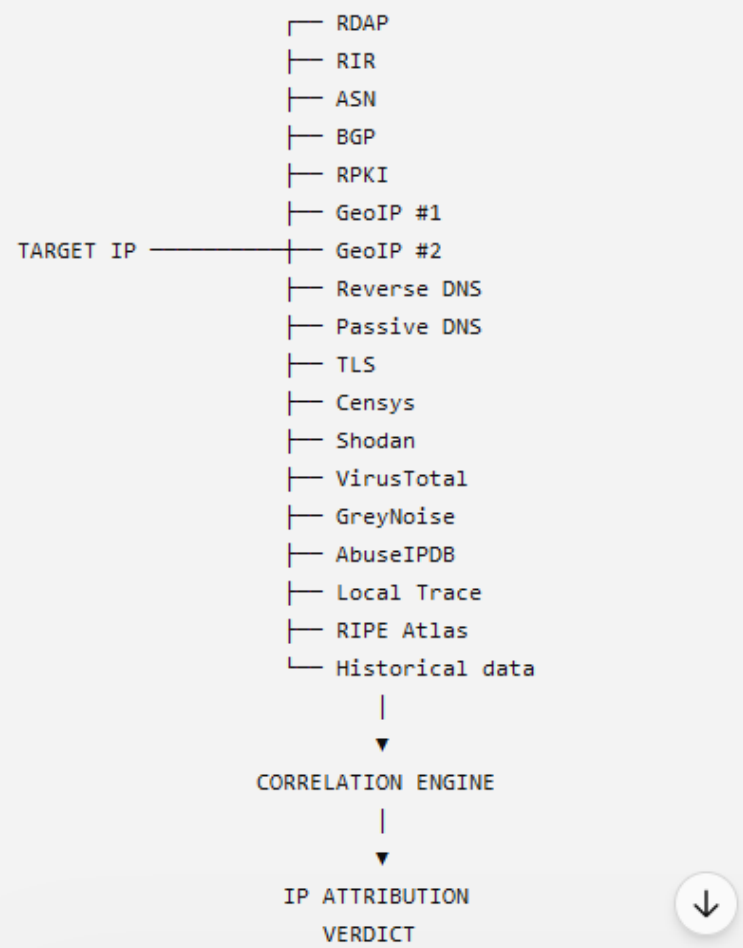
16. Le moteur de corrélation serait le cœur du produit

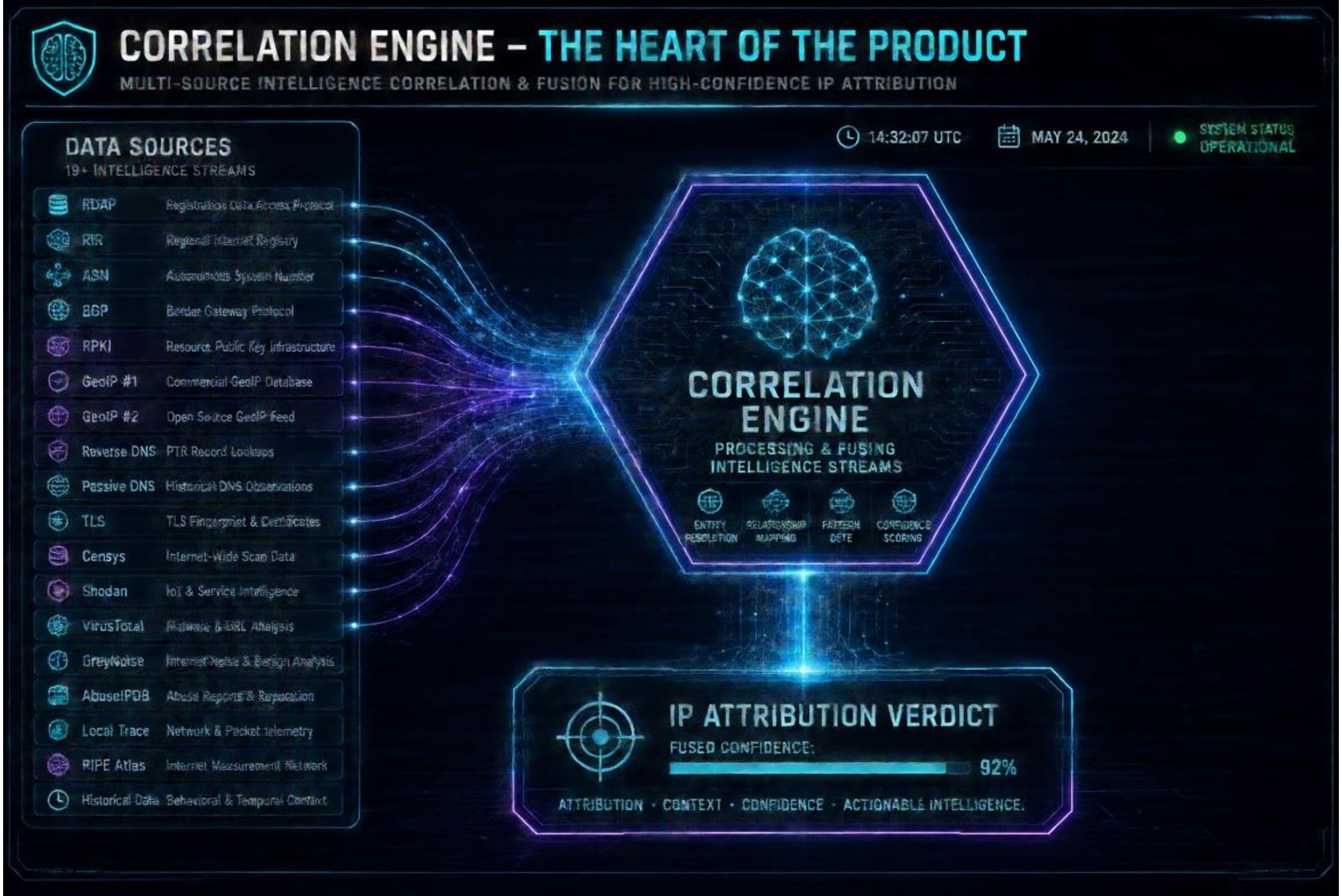
Je ne veux surtout pas :

```
API MaxMind → afficher résultat
```

Ce serait sans intérêt.

Je veux quelque chose du type :




CORRELATION ENGINE – THE HEART OF THE PRODUCT
MULTI-SOURCE INTELLIGENCE CORRELATION & FUSION FOR HIGH-CONFIDENCE IP ATTRIBUTION
DATA SOURCES
19+ INTELLIGENCE STREAMS
RDAP
RIR
ASN
BGP
RPKI
GeoIP #1
GeoIP #2
Reverse DNS
Passive DNS
TLS
Censys
Shodan
VirusTotal
GreyNoise
AbuseIPDB
Local Trace
RIPE Atlas
Historical Data
14:32:07 UTC
MAY 24, 2024
SYSTEM STATUS
OPERATIONAL
CORRELATION ENGINE
PROCESSING & FUSING INTELLIGENCE STREAMS
IP ATTRIBUTION VERDICT
FUSED CONFIDENCE:
92%
ATTRIBUTION · CONTEXT · CONFIDENCE · ACTIONABLE INTELLIGENCE.

17. Et surtout : un Confidence Engine

Chaque donnée doit avoir :

VALUE

SOURCE

TIMESTAMP

CONFIDENCE

Par exemple :

> **Country: Netherlands — 99%**

> Evidence: MaxMind + IPinfo + RIR + ASN + traceroute.

Mais :

> **City: Amsterdam — 54%**

> Conflicting evidence: MaxMind Amsterdam / PTR AMS / RTT compatible; DB-IP Haarlem.

Cela empêchera notre produit de raconter des absurdités avec une précision artificielle.

18. Dashboard que je vois pour Security Analyzer

Je ferais une énorme zone :

DEEP IP INTELLIGENCE

avec simplement :

IP ADDRESS

`[_____________________]`

ANALYZE IP

Puis des onglets :

`OVERVIEW | GEO | OWNERSHIP | ASN/BGP | TRACE | DNS | TLS | SERVICES | REPUTATION | HISTORY | EVIDENCE`

Et en Overview :

IP ATTRIBUTION SCORE

91 / 100

NETWORK

`ASxxxx — OVH / AWS / Orange / Telefonica / etc.`

LOCATION

🌍 Spain
📍 Madrid
⭕ Accuracy ±40 km

LOCATION

Ignorer et passer au contenu

🌍 Spain
📍 Madrid
⭕ Accuracy ±40 km

CLASSIFICATION

`DATACENTER`

PRIVACY

`VPN: NO`

`PROXY: NO`

`TOR: NO`

REPUTATION

`LOW RISK`

ROUTING

`RPKI VALID`

TRACE

`14 HOPS`

CONFIDENCE

`HIGH`

Visuellement, cela peut être **très impressionnant pour une démonstration du Security Analyzer**.

Et je séparerais le produit en trois profondeurs

QUICK LOOKUP — quelques secondes, quasi exclusivement passif : RDAP, ASN, BGP, GeoIP, DNS, réputation.

DEEP ANALYSIS — interrogation de toutes nos sources, certificats, historique, Internet exposure, multi-database correlation.

FORENSIC TRACE — mesures réseau autorisées, multi-vantage traceroutes, analyse hop par hop, BGP historique et corrélation géographique.

Cela donne une progression visible à l'utilisateur au lieu d'une page qui attend pendant que 20 moteurs travaillent.

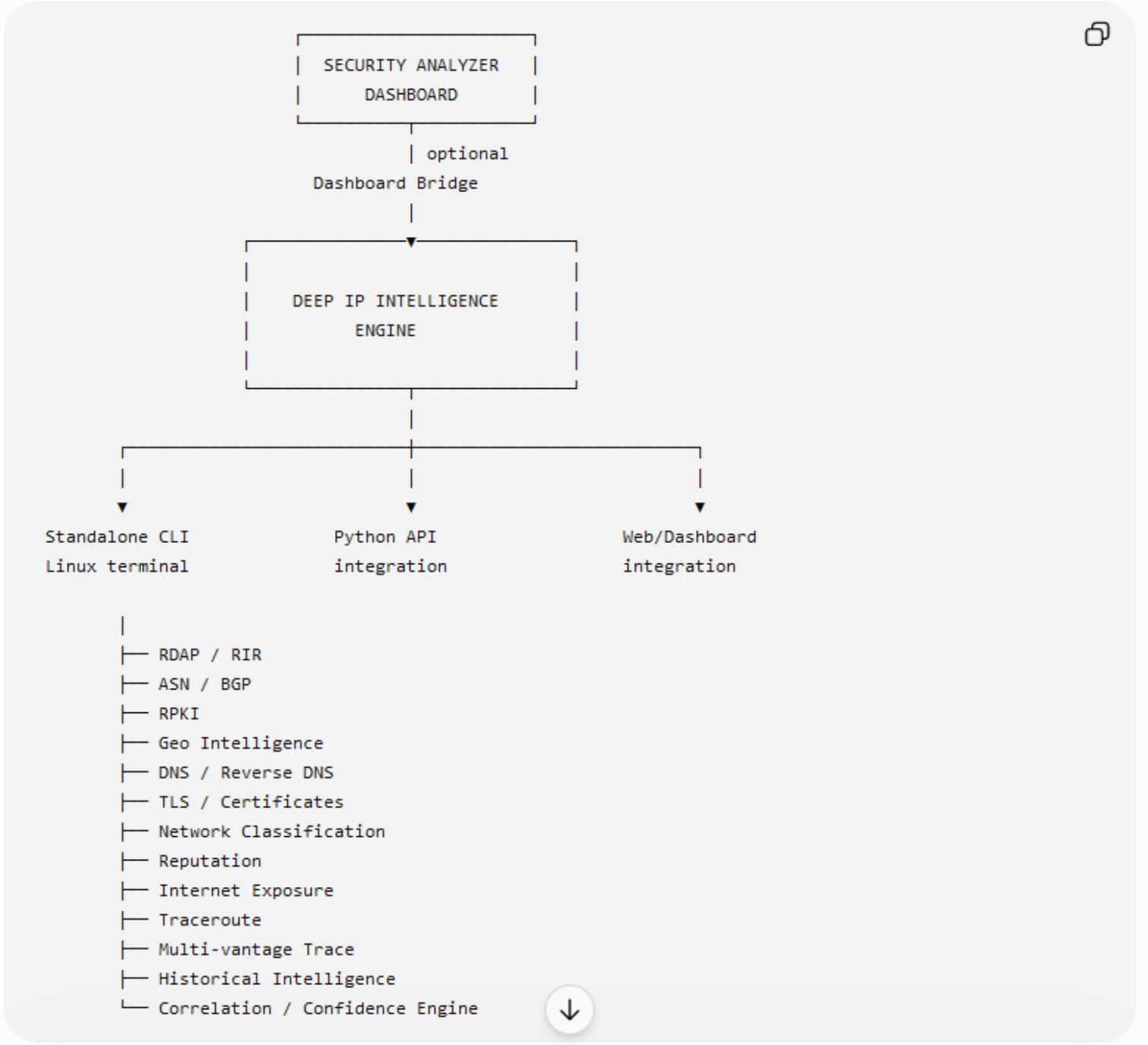
Un point d'architecture important

Je conserverais parfaitement l'esprit du **Security Analyzer standalone** : Python + nos vues HTML/JS + notre orchestrateur. Les APIs extérieures seraient des **sources de renseignement facultatives**, pas des dépendances architecturales. Le moteur de base continuerait donc à fonctionner même sans Shodan, Censys ou VirusTotal.

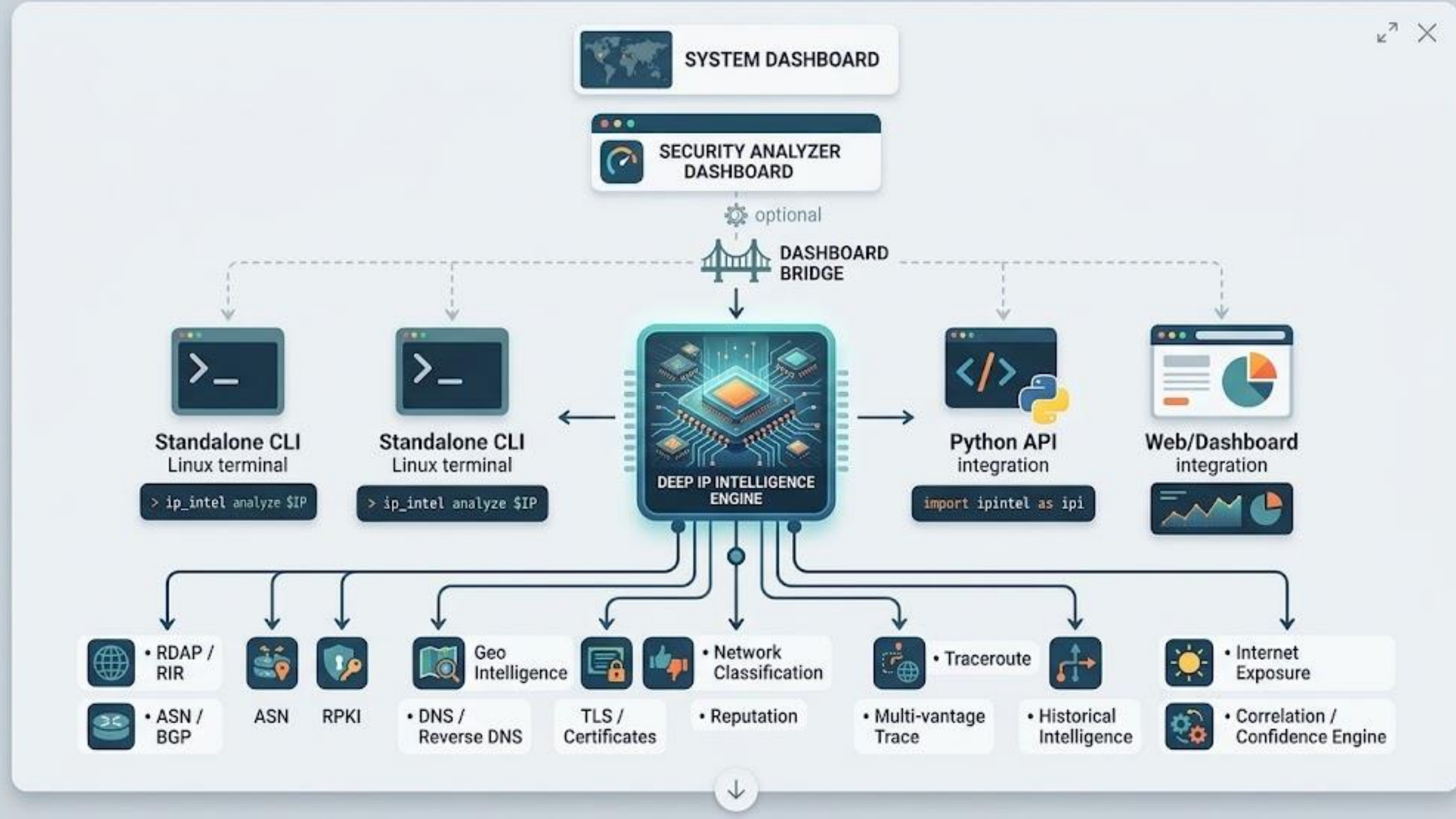
Et conformément à notre méthode de travail du Security Analyzer, je **ne vais pas inventer maintenant une nouvelle série de noms de patches** avant d'avoir fixé cette architecture. En revanche, le développement peut très bien être structuré ensuite en **lots de trois**, en commençant par le moteur IP/RDAP/ASN-BGP, puis Geo/DNS, puis traceroute/corrélation.

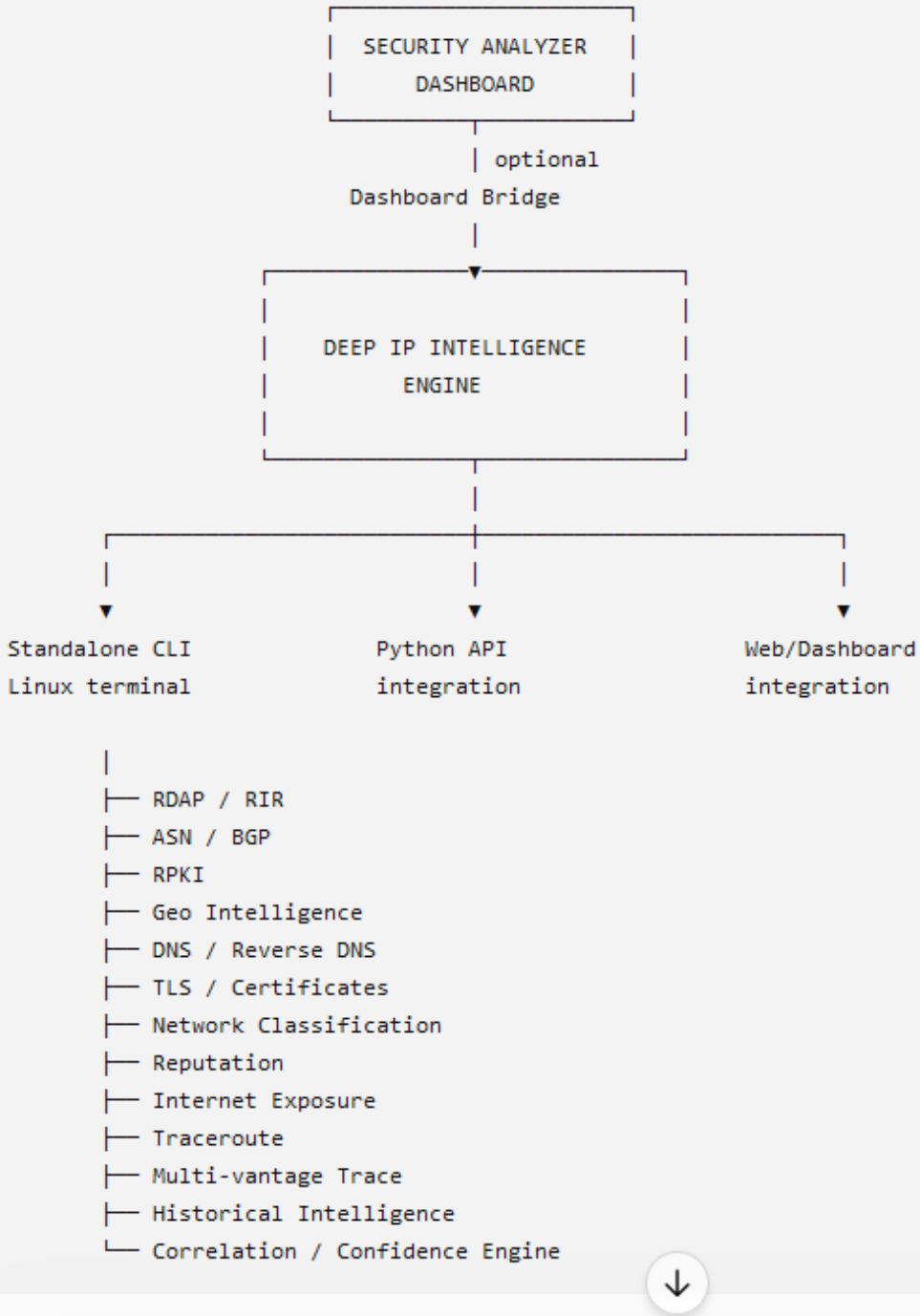
À mon sens, ce module mérite vraiment d'être poussé loin : **pas un "IP Lookup" mais un véritable moteur d'IP Intelligence**, capable de répondre à quatre questions distinctes : **qui possède l'IP, qui l'annonce réellement, où l'infrastructure semble être, et que savons-nous de son historique et de son comportement réseau.**

ROADMAP IP ANALYZER



ROADMAP PATCHS


SYSTEM DASHBOARD
SECURITY ANALYZER DASHBOARD
optional
DASHBOARD BRIDGE
Standalone CLI
Linux terminal
> ip_intel analyze $IP
Standalone CLI
Linux terminal
> ip_intel analyze $IP
DEEP IP INTELLIGENCE ENGINE
Python API
integration
import ipintel as ipi
Web/Dashboard
integration
• RDAP / RIR
• ASN / BGP
ASN
RPKI
Geo Intelligence
• DNS / Reverse DNS
TLS / Certificates
• Network Classification
• Reputation
• Traceroute
• Multi-vantage Trace
• Historical Intelligence
• Internet Exposure
• Correlation / Confidence Engine


SECURITY ANALYZER
DASHBOARD
optional
Dashboard Bridge
DEEP IP INTELLIGENCE
ENGINE
Standalone CLI
Linux terminal
Python API
integration
Web/Dashboard
integration
RDAP / RIR
ASN / BGP
RPKI
Geo Intelligence
DNS / Reverse DNS
TLS / Certificates
Network Classification
Reputation
Internet Exposure
Traceroute
Multi-vantage Trace
Historical Intelligence
Correlation / Confidence Engine

Batch	Patches	Objectif
BATCH 1 — FOUNDATION	IP-INTEL-001A / 001B / 001C	Construire le cœur standalone et l'orchestrateur
BATCH 2 — OWNERSHIP	IP-INTEL-002A / 002B / 002C	RIR, RDAP, propriétaire et attribution
BATCH 3 — BGP	IP-INTEL-003A / 003B / 003C	ASN, routing, BGP, RPKI
BATCH 4 — GEO	IP-INTEL-004A / 004B / 004C	Géolocalisation multi-sources et classification
BATCH 5 — DNS/TLS	IP-INTEL-005A / 005B / 005C	DNS, reverse DNS, domaines et certificats
BATCH 6 — EXPOSURE	IP-INTEL-006A / 006B / 006C	Services observés et exposition Internet
BATCH 7 — THREAT INTEL	IP-INTEL-007A / 007B / 007C	Réputation et renseignements cyber
BATCH 8 — TRACE	IP-INTEL-008A / 008B / 008C	Traceroute avancé et enrichissement des hops
BATCH 9 — GLOBAL TRACE	IP-INTEL-009A / 009B / 009C	Mesures multi-points et analyse géographique
BATCH 10 — CORRELATION	IP-INTEL-010A / 010B / 010C	Intelligence fusion, contradictions, confiance
BATCH 11 — HISTORY	IP-INTEL-011A / 011B / 011C	Historique IP et timeline
BATCH 12 — DASHBOARD	IP-INTEL-012A / 012B / 012C	Intégration spectaculaire au Security Analyzer
BATCH 13 — REPORTING	IP-INTEL-013A / 013B / 013C	Rapports, JSON, export et preuves
BATCH 14 — HARDENING	IP-INTEL-014A / 014B / 014C	Performance, résilience, tests et production

AGENDA DES BATCHS

- BATCH 1 — FOUNDATION
- BATCH 2 — OWNERSHIP
- BATCH 3 — ASN / BGP / RPKI
- BATCH 4 — GEO INTELLIGENCE
- BATCH 5 — DNS & TLS INTELLIGENCE
- BATCH 6 — INTERNET EXPOSURE
- BATCH 7 — THREAT INTELLIGENCE
- BATCH 8 — DEEP TRACE
- BATCH 9 — MULTI-VANTAGE TRACE
- BATCH 10 — CORRELATION ENGINE
- BATCH 11 — HISTORICAL INTELLIGENCE
- BATCH 12 — SECURITY ANALYZER DASHBOARD
- BATCH 13 — REPORTING
- BATCH 14 — HARDENING

IP INTELLIGENCE SUMMARY

IP	185.xxx.xxx.xxx
RIR	RIPE NCC
Prefix	185.xxx.xxx.0/24
ASN	ASxxxxx
Owner	Example Hosting Ltd
Operator	Example Cloud Europe

NETWORK TYPE	
Datacenter / Hosting	98%

LOCATION	
Spain	99%
Madrid Region	91%
Madrid	67%
Estimated uncertainty	±45 km

ROUTING	
RPKI	VALID
BGP consistency	HIGH
Anycast	UNLIKELY

IDENTITY SIGNALS	
PTR	xxx.example.net
TLS domains	14
Associated domains	27

EXPOSURE	
Observed services	5

TRACE	
Hops	13
AS networks crossed	6
Probable final POP	Madrid

LES 3 NIVEAUX D'ANALYSE

QUICK doit être extrêmement rapide et essentiellement passif :

```
RDAP
Owner
ASN
Prefix
Geo
Reverse DNS
Network Type
Basic Reputation
```

DEEP lance pratiquement tout ce qui est passif :

```
Quick +
BGP
RPKI
DNS
TLS
Exposure
Threat Intelligence
History
Correlation
```

FORENSIC TRACE ajoute les mesures réseau :

```
Deep +
Traceroute
Hop enrichment
Remote probes
Route comparison
Latency inference
Anycast detection
Geo consistency
```

QUICK doit être extrêmement rapide et essentiellement passif :

- RDAP
- Owner
- ASN
- Prefix
- Geo
- Reverse DNS
- Network Type
- Basic Reputation

DEEP lance pratiquement tout ce qui est passif :

- → Quick +
- BGP
- RPKI
- DNS
- TLS
- Exposure
- Threat Intelligence
- History
- Correlation

FORENSIC TRACE ajoute les mesures réseau :

- → Deep +
- Traceroute
- Hop enrichment
- Remote probes
- Route comparison
- Latency inference
- Anycast detection
- Geo consistency

BATCH 1



IP-INTEL-001A — IP Input & Validation Core

Le programme devra reconnaître automatiquement :

IPv4, IPv6, IPv4-mapped IPv6, IP publique, privée, loopback, multicast, reserved, link-local, documentation ranges et autres plages particulières.

Il effectuera également une normalisation systématique.

Exemple futur :

```bash
python3 ip_intel.py 185.xxx.xxx.xxx
```

ou :

```bash
python3 ip_intel.py 185.xxx.xxx.xxx --deep
```

IP-INTEL-001B — Analyzer Orchestrator

Création du cœur capable de lancer les différents analyseurs indépendamment.

Concept :

```
TARGET
   |
   ├── registry
   ├── bgp
   ├── geo
   ├── dns
   ├── tls
   ├── reputation
   ├── exposure
   └── trace
```

Chaque analyseur devra retourner une structure standardisée :

JSON

```json
{
    "analyzer": "rdap",
    "status": "success",
    "duration_ms": 320,
    "data": {},
    "evidence": [],
    "warnings": []
}
```

IP-INTEL-001C — Standalone Linux CLI

Première véritable version utilisable indépendamment du Security Analyzer.

Modes prévus :

```
--quick
--deep
--trace
--active
--json
--verbose
```

Avec une première sortie console propre et lisible.

À la fin du Batch 1 : le produit existe déjà en standalone.

BATCH 2



IP Ownership Pipeline

1. IP



2. IANA Bootstrap



3. RIR autoritaire
(RIPE, ARIN, APNIC style)



4. RDAP



JSON lookup

5. Ownership extraction



6. Ownership verdict



IP-INTEL-002A — RDAP / RIR Analyzer

Interrogation automatique du bon registre :

ARIN, RIPE NCC, APNIC, LACNIC, AFRINIC.

Extraction :

```
IP range
CIDR
RIR
NetName
Organization
Registration
Last update
Status
Abuse contacts
Technical contacts
```

IP-INTEL-002B — Network Ownership Analyzer

Différencier clairement :

```
REGISTERED OWNER
ALLOCATED TO
CURRENT OPERATOR
HOSTING PROVIDER
BGP ORIGIN
```

C'est essentiel car ils peuvent être différents.

IP-INTEL-002C — Ownership Verdict

Le moteur synthétise les données :

```
INFRASTRUCTURE OWNER
OVH SAS

NETWORK OPERATOR
OVHcloud

RIR
RIPE NCC

CONFIDENCE
98%
```

oneill_1404

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version           : 0.2.0
Status            : OK
Profile           : quick
Target            : 8.8.8.8
Address family    : IPv4
Category          : public-global
Category detail   : Public globally routable address
Globally routable : yes
Reverse pointer   : 8.8.8.8.in-addr.arpa
Duration          : 451.467 ms

Analyzers
---------
ip-input             OK       0.021 ms
rdap                 OK       451.434 ms
  warning: Current operator and BGP origin are intentionally unconfirmed until Batch 3.

RDAP / RIR
----------
RIR               : ARIN
IP range          : 8.8.8.0 - 8.8.8.255
CIDR              : 8.8.8.0/24
NetName           : GOGL
Organization      : Google LLC
Registration      : 2023-12-28T17:24:33-05:00
Last update       : 2023-12-28T17:24:56-05:00
Status            : active
Abuse contacts    : Google Inc. <network-abuse@google.com>
Technical contacts: Google LLC <arin-contact@google.com>

Network ownership
-----------------
REGISTERED OWNER  : Google LLC
ALLOCATED TO      : Google LLC
CURRENT OPERATOR  : unconfirmed - BGP confirmation in Batch 3
HOSTING PROVIDER  : unconfirmed - classification in Batch 4
BGP ORIGIN        : not queried - Batch 3

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : Google LLC
NETWORK OPERATOR     : Google LLC [BGP unconfirmed]
RIR                  : ARIN
CONFIDENCE           : 95%

Batch 2 RDAP/RIR ownership intelligence is ready. ASN/BGP enrichment arrives in Batch 3.
ubuntu@ip-172-31-42-227:/home/gon2000fr$
```

IDEO-Lab

DEEP IP INTELLIGENCE ANALYZER

New Scan

Metadata

Version	0.2.0	Address Family	IPv4
Status	Online	Profile	quick
Target	**8.8.8.8**	Reverse familly	
Category family	IPv4	Public-global	
Category detail	yes	Public globally routable arpa	
Duration	**451.467 ms**		

Analyzers

ip-input	100%	0.021 ms
rdap	100%	451.434 ms

Operator and BGP origin data unconfirmed until Batch 3.

RDAP / RIR Registry

Field	Value
RIR	ARIN
IP range	8.8.8.0 - 8.8.8.255
CIDR	8.8.8.0/24
NetName	GOGL
Organization	Google LLC
Registration	2023-12-28T7:24:33-05:00
Last update	2023-12-28T7:24:56-05:00
Status	active
Abuse contacts	Google Inc. <network-abuse.com>
Technical contacts	arin-contact@google.com>

Network Ownership

Registered Owner	**Google LLC**
Allocated To	**Google LLC**
Current Operator	Unconfirmed - BGP check in Batch 3
Hosting Provider	Classification in Batch 4
BGP Origin	Not Queried

Verdict



Verified 95%

Confidence Score

Infrastructure Owner **Google LLC**

Network Operator **Google LLC [BGP Unconfirmed]**

RIR **ARIN**

Batch 2 (RDAP/RIR) complete. ASN/BGP enrichment arrives in Batch 3.

Metadata

Online

Status	IDEO-Lab
Target IP	8.8.8.8
Progress	192.0.2.0 / 24
Confirmt Date	2023-02-38 01:07:13 (GBUTC)
Last untimd	2023-02-05 10:27:56 UTC

Analyzers

ip-input 00:35 / 15.7ms

rdap 37:45 / 16.1ms

Timing: 0.13ms

Timing: 21.31ms

⚠ Operator and BGP origin data unconfirmed until Batch 3.

RDAP / RIR Registry

RIR	ARIN
IP range	192.0.2.0 /24
CIDR	192.0.2.0 /24
NetName	ARIN-Netnan
Organization	ARIN Lab Organization Inc.
Dates	2022-02-26 16:39:54 - 2023-02-07 . 2021-02-31
Status	Confidenc: 98%
Contacts	emails:wane@email.com · emailszwum@gmail.com · nutomortlawn@gmail.com

Network Ownership

- IDEO-Lab
  Network Owner
- Network Owner
  Allocation · Contacts
- Network Operator
  Network Operator
- Scan Sample
  None

Verdict

95%

Confidence Score

STAVBED

Infrastructure Owner
Infrastructure Owner

Network Operator
Network Operator

Batch 2 (RDAP/RIR) complete. ASN/BGP enrichment arrives in Batch 3.

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version           : 0.2.0
Status            : OK
Profile           : quick
Target            : 1.1.1.1
Address family    : IPv4
Category          : public-global
Category detail   : Public globally routable address
Globally routable : yes
Reverse pointer   : 1.1.1.1.in-addr.arpa
Duration          : 177.945 ms

Analyzers
---------
ip-input             OK       0.021 ms
rdap                 OK       177.909 ms
  warning: Current operator and BGP origin are intentionally unconfirmed until Batch 3.

RDAP / RIR
----------
RIR               : APNIC
IP range          : 1.1.1.0 - 1.1.1.255
CIDR              : 1.1.1.0/24
NetName           : APNIC-LABS
Organization      : APNIC Research and Development
Registration      : 2011-08-10T23:12:35Z
Last update       : 2023-04-26T22:57:58Z
Status            : active
Abuse contacts    : IRT-APNICRANDNET-AU <helpdesk@apnic.net>
Technical contacts: APNICRANDNET Infrastructure Contact <research@apnic.net>

Network ownership
-----------------
REGISTERED OWNER  : APNIC Research and Development
ALLOCATED TO      : APNIC Research and Development
CURRENT OPERATOR  : unconfirmed - BGP confirmation in Batch 3
HOSTING PROVIDER  : unconfirmed - classification in Batch 4
BGP ORIGIN        : not queried - Batch 3

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : APNIC Research and Development
NETWORK OPERATOR     : APNIC Research and Development [BGP unconfirmed]
RIR                  : APNIC
CONFIDENCE           : 95%

Batch 2 RDAP/RIR ownership intelligence is ready. ASN/BGP enrichment arrives in Batch 3.
```

IDEO-Lab

DEEP IP INTELLIGENCE ANALYZER

New Scan



Metadata

Version	0.2.0
Status	Online/OK
Profile	Quick
Target	1.1.1.1
Address family	IPv4
Category	public-global
Category detail	Public globally routable address
Globally routable	Yes
Reverse pointer	1.1.1.1.in-addr.arpa
Duration	177.945 ms

Analyzers

ip-input	100%	0.021 ms
rdap	100%	177.909 ms
BGP		Pending Batch 3

⚠ Current operator and BGP origin unconfirmed until Batch 3

RDAP / RIR Registry

RIR	APNIC
IP range	1.1.1.0 - 1.1.1.255
CIDR	1.1.1.0/24
NetName	APNIC-LABS
Organization	APNIC Research and Development
Registration	2011-08-10T23:12:35Z
Last update	2023-04-26T22:57:58Z
Status	Active
Abuse contacts	IRT-APNICRANDNET-AU helpdesk@apnic.net
Technical contacts	APNICRANDNET Infrastructure Contact

Network Ownership & Verdict

REGISTERED OWNER	APNIC Research and Development
ALLOCATED TO	APNIC Research and Development

Ownership Verdict

INFRASTRUCTURE OWNER	APNIC Research and Development
NETWORK OPERATOR	APNIC Research and Development [BGP unconfirmed]
RIR	APNIC
CONFIDENCE	**95%**



Batch 2 RDAP/RIR ownership intelligence is ready. ASN/BGP enrichment arrives in Batch 3.

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version            : 0.2.0
Status             : OK
Profile            : quick
Target             : 200.160.2.3
Address family     : IPv4
Category           : public-global
Category detail    : Public globally routable address
Globally routable  : yes
Reverse pointer    : 3.2.160.200.in-addr.arpa
Duration           : 1589.663 ms

Analyzers
---------
ip-input              OK       0.022 ms
rdap                  OK       1589.624 ms
  warning: Current operator and BGP origin are intentionally unconfirmed until Batch 3.

RDAP / RIR
----------
RIR                : LACNIC
IP range           : 200.160.0.0 - 200.160.15.255
CIDR               : 200.160.0.0/20
NetName            : 22817
Organization       : NÃºcleo de Inf. e Coord. do Ponto BR - NIC.BR
Registration       : 2001-10-16T12:00:00Z
Last update        : 2013-03-07T23:00:38Z
Status             : active
Abuse contacts     : Frederico Augusto de Carvalho Neves <fneves@registro.br>
Technical contacts: Frederico Augusto de Carvalho Neves <fneves@registro.br>; Frederico August
ho Neves <fneves@registro.br>

Network ownership
-----------------
REGISTERED OWNER   : NÃºcleo de Inf. e Coord. do Ponto BR - NIC.BR
ALLOCATED TO       : NÃºcleo de Inf. e Coord. do Ponto BR - NIC.BR
CURRENT OPERATOR   : unconfirmed - BGP confirmation in Batch 3
HOSTING PROVIDER   : unconfirmed - classification in Batch 4
BGP ORIGIN         : not queried - Batch 3

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : NÃºcleo de Inf. e Coord. do Ponto BR - NIC.BR
NETWORK OPERATOR     : NÃºcleo de Inf. e Coord. do Ponto BR - NIC.BR [BGP unconfirmed]
RIR                  : LACNIC
CONFIDENCE           : 95%

Batch 2 RDAP/RIR ownership intelligence is ready. ASN/BGP enrichment arrives in Batch 3.
```

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version            : 0.2.0
Status             : OK
Profile            : quick
Target             : 196.216.2.1
Address family     : IPv4
Category           : public-global
Category detail    : Public globally routable address
Globally routable  : yes
Reverse pointer    : 1.2.216.196.in-addr.arpa
Duration           : 733.403 ms

Analyzers
---------
ip-input             OK       0.022 ms
rdap                 OK       733.365 ms
  warning: Current operator and BGP origin are intentionally unconfirmed until Batch 3.

RDAP / RIR
----------
RIR                : AFRINIC
IP range           : 196.216.2.0 - 196.216.3.255
CIDR               : 196.216.2.0/23
NetName            : ORG-AFNC1-AFRINIC
Organization       : African Network Information Center - (AfriNIC) Ltd
Registration       : 2005-02-21T15:30:00Z
Last update        : 2020-08-18T12:16:00Z
Status             : active
Abuse contacts     : -
Technical contacts: Infrastructure Team <sysadmin@afrinic.net>; CTO AFRINIC <cto@afrinic.net>

Network ownership
-----------------
REGISTERED OWNER   : African Network Information Center - (AfriNIC) Ltd
ALLOCATED TO       : African Network Information Center - (AfriNIC) Ltd
CURRENT OPERATOR   : unconfirmed - BGP confirmation in Batch 3
HOSTING PROVIDER   : unconfirmed - classification in Batch 4
BGP ORIGIN         : not queried - Batch 3

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : African Network Information Center - (AfriNIC) Ltd
NETWORK OPERATOR     : African Network Information Center - (AfriNIC) Ltd [BGP unconfirmed]
RIR                  : AFRINIC
CONFIDENCE           : 95%

Batch 2 RDAP/RIR ownership intelligence is ready. ASN/BGP enrichment arrives in Batch 3.
```

BATCH 3



IP-INTEL-003A — ASN Intelligence

Détermination de :

```
ASN
ASN name
ASN organization
Country
Prefixes
Allocated IP count
Upstreams
Peers
```

IP-INTEL-003B — BGP Route Intelligence

Analyse :

```
Origin ASN
BGP prefix
AS path
Transit networks
Peers
Route visibility
Announcements
Withdrawals
```

On commence ici à reconstruire **la véritable position de l'IP dans Internet.**

IP-INTEL-003C — RPKI & Routing Security

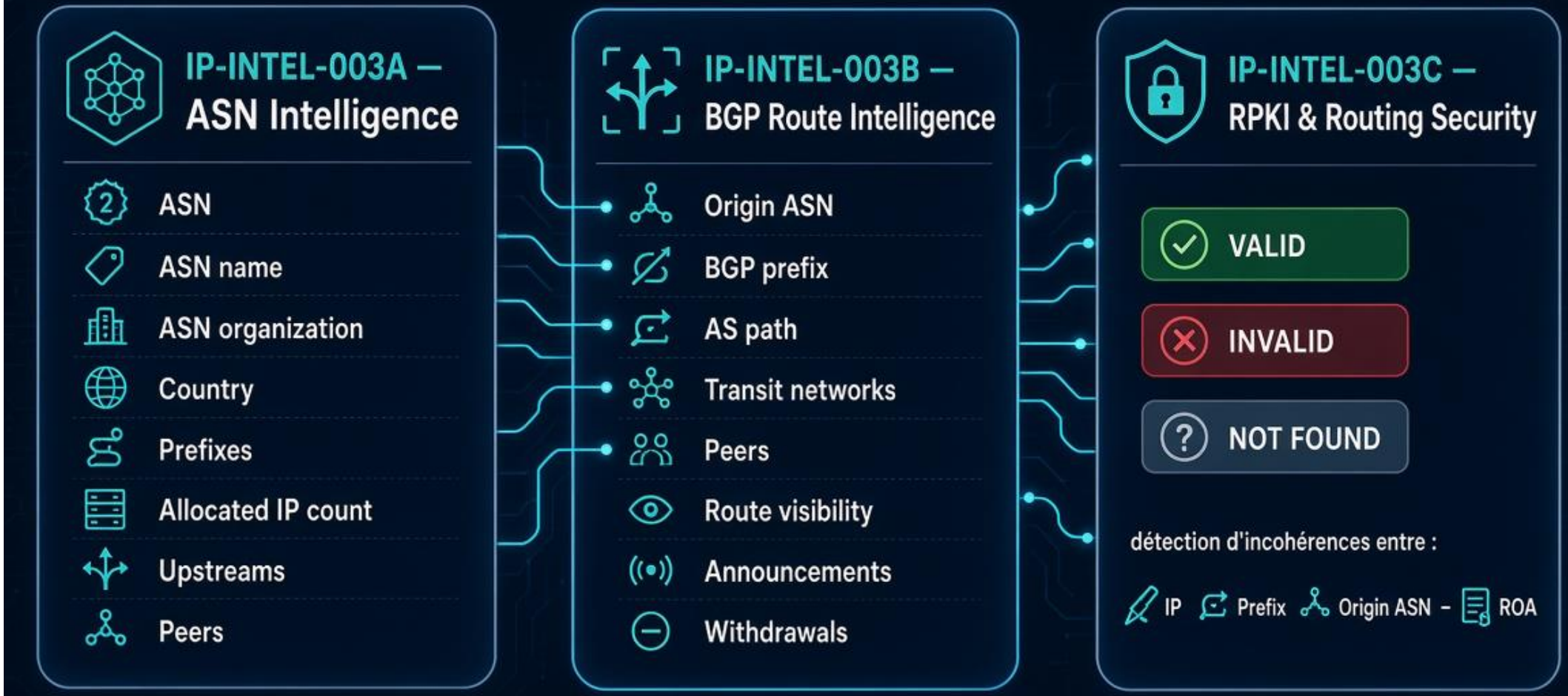
État :

```
VALID
INVALID
NOT FOUND
```

avec détection des incohérences entre :

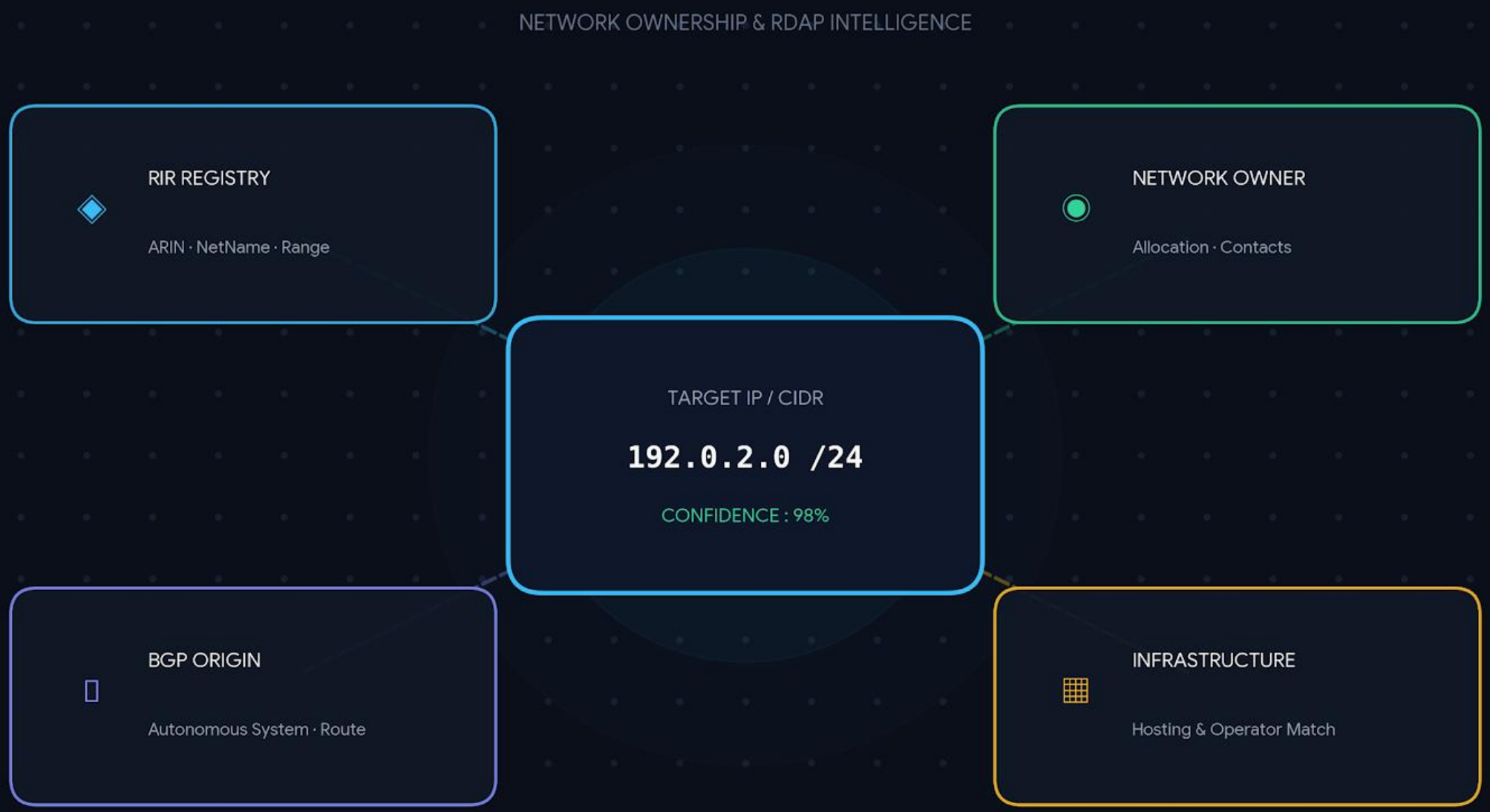
```
IP
Prefix
Origin ASN
ROA
```

IP-INTEL — Position réelle de l'IP sur Internet



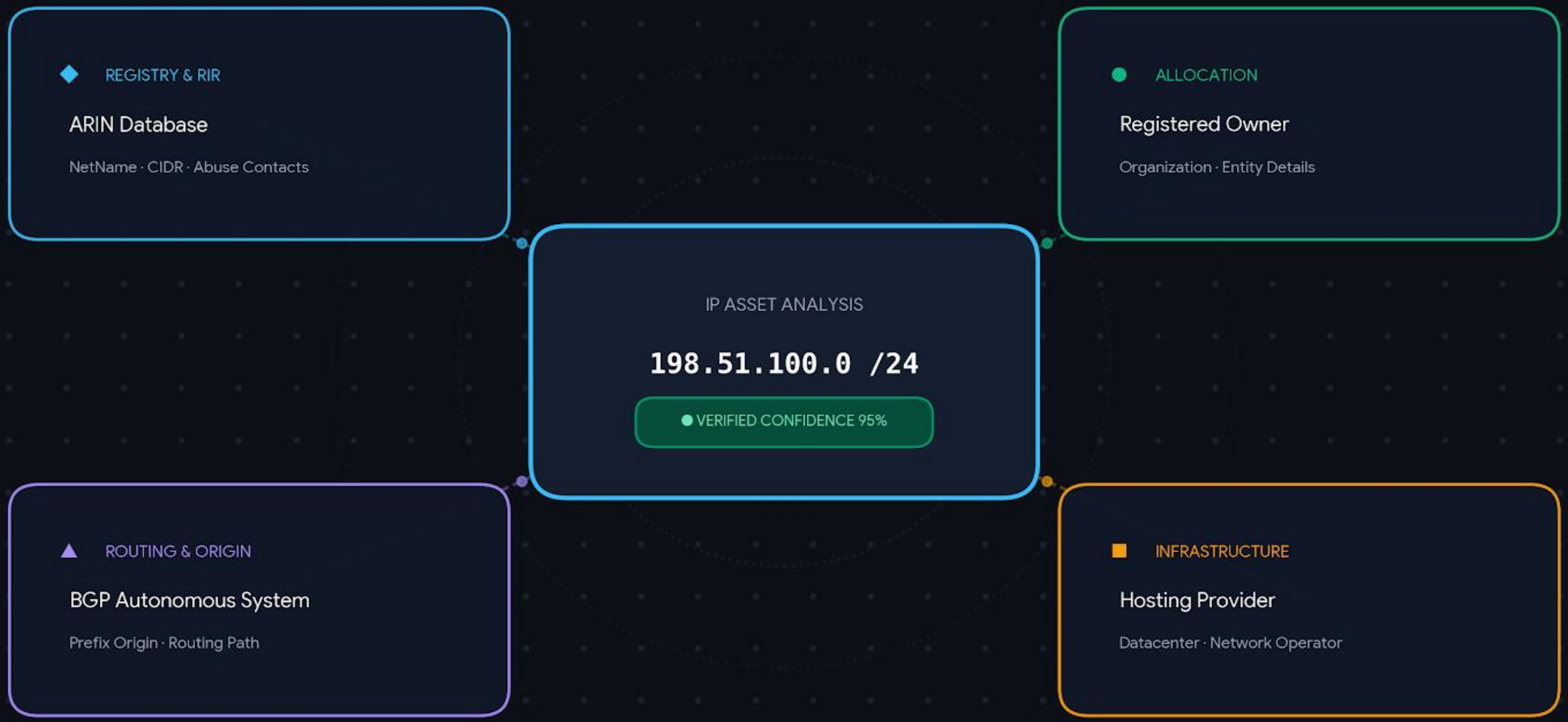
On commence ici à reconstruire la véritable position de l'IP dans Internet.

```
Analyzers
---------
ip-input              OK
rdap                  OK

RDAP / RIR
----------
RIR               : ARIN
IP range          : ...
CIDR              : ...
NetName           : ...
Organization      : ...
Registration      : ...
Last update       : ...
Status            : ...
Abuse contacts    : ...
Technical contacts: ...

Network ownership
-----------------
REGISTERED OWNER  : ...
ALLOCATED TO      : ...
CURRENT OPERATOR  : unconfirmed - BGP corfirmation in Batch 3
HOSTING PROVIDER  : unconfirmed - classification in Batch 4
BGP ORIGIN        : not queried - Batch 3

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : ...
NETWORK OPERATOR     : ... [BGP unconfirmed]
RIR                  : ARIN
CONFIDENCE           : xx%
```


NETWORK OWNERSHIP & RDAP INTELLIGENCE
RIR REGISTRY
ARIN · NetName · Range
NETWORK OWNER
Allocation · Contacts
TARGET IP / CIDR
192.0.2.0 /24
CONFIDENCE : 98%
BGP ORIGIN
Autonomous System · Route
INFRASTRUCTURE
Hosting & Operator Match

RDAP & NETWORK OWNERSHIP PROFILING

Automated IP Allocation · BGP Route · Infrastructure Mapping



on devrait désormais avoir cinq moteurs :

```
Analyzers
---------
ip-input            OK
rdap                OK
asn                 OK
bgp                 OK
rpki                OK
```

puis quelque chose dans cet esprit :

```
Network ownership
-----------------
REGISTERED OWNER  : Google LLC
ALLOCATED TO      : Google LLC
CURRENT OPERATOR  : Google LLC
HOSTING PROVIDER  : unconfirmed - classification in Batch 4
BGP ORIGIN        : AS15169
```

puis :

```
ASN intelligence
----------------
Routed prefix     : 8.8.8.0/24
Origin ASN(s)     : AS15169
Multi-origin      : no
AS15169           : Google LLC
```

IP Intelligence — Cinq moteurs

Analyse complète d'une adresse IP

1. ip-input OK
2. rdap OK
3. asm OK
4. bgp OK
5. rpki OK

Network ownership

REGISTERED OWNER	Google LLC
ALLOCATED TO	Google LLC
CURRENT OPERATOR	Google LLC
HOSTING PROVIDER	unconfirmed — Batch 4
BGP ORIGIN	AS15169

ASN intelligence

Routed prefix	8.8.8.0/24
Origin ASN(s)	AS15169
Multi-origin	no
AS15169	Google LLC

IP Intelligence — Position de l'IP

ASN · BGP · RPKI

ASN intelligence

Routed prefix :	8.8.8.0/24
Origin ASN(s) :	AS15169
Multi-origin :	no
AS15169 :	Google LLC

BGP route intelligence

Observed origin :	AS15169
Origin consistent :	yes
Routes observed :	•••
Unique AS paths :	•••
RIS collectors :	•••
Path-adjacent AS :	•••

RPKI / routing security

RPKI verdict

VALID ✓ INVALID ✗ NOT FOUND ?

AS15169 : •••

IDEO-Lab

DEEP IP INTELLIGENCE ANALYZER

New Scan



Metadata

Version	0.2.0
Status	Online/OK
Profile	Quick
Target	1.1.1.1
Address family	IPv4
Category	public-global
Category detail	Public globally routable address
Globally routable	Yes
Reverse pointer	1.1.1.1.in-addr.arpa
Duration	177.945 ms

Analyzers

ip-input	100%	0.021 ms
rdap	100%	177.909 ms
BGP		Pending Batch 3

⚠ Current operator and BGP origin unconfirmed until Batch 3

RDAP / RIR Registry

RIR	APNIC
IP range	1.1.1.0 - 1.1.1.255
CIDR	1.1.1.0/24
NetName	APNIC-LABS
Organization	APNIC Research and Development
Registration	2011-08-10T23:12:35Z
Last update	2023-04-26T22:57:58Z
Status	Active
Abuse contacts	IRT-APNICRANDNET-AU helpdesk@apnic.net
Technical contacts	APNICRANDNET Infrastructure Contact

Network Ownership & Verdict

REGISTERED OWNER	APNIC Research and Development
ALLOCATED TO	APNIC Research and Development

Ownership Verdict

INFRASTRUCTURE OWNER	APNIC Research and Development
NETWORK OPERATOR	APNIC Research and Development [BGP unconfirmed]
RIR	APNIC
CONFIDENCE	**95%**



Batch 2 RDAP/RIR ownership intelligence is ready. ASN/BGP enrichment arrives in Batch 3.

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version           : 0.3.0
Status            : OK
Profile           : quick
Target            : 1.1.1.1
Address family    : IPv4
Category          : public-global
Category detail   : Public globally routable address
Globally routable : yes
Reverse pointer   : 1.1.1.1.in-addr.arpa
Duration          : 1572.826 ms

Analyzers
---------
ip-input             OK       0.022 ms
rdap                 OK       363.927 ms
  warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers correlate those signals lat
er in the run.
asn                  OK       726.051 ms
bgp                  OK       395.641 ms
rpki                 OK       87.137 ms

RDAP / RIR
----------
RIR               : APNIC
IP range          : 1.1.1.0 - 1.1.1.255
CIDR              : 1.1.1.0/24
NetName           : APNIC-LABS
Organization      : APNIC Research and Development
Registration      : 2011-08-10T23:12:35Z
Last update       : 2023-04-26T22:57:58Z
Status            : active
Abuse contacts    : IRT-APNICRANDNET-AU <helpdesk@apnic.net>
Technical contacts: APNICRANDNET Infrastructure Contact <research@apnic.net>

Network ownership
-----------------
REGISTERED OWNER  : APNIC Research and Development
ALLOCATED TO      : APNIC Research and Development
CURRENT OPERATOR  : CLOUDFLARENET - Cloudflare, Inc.
HOSTING PROVIDER  : unconfirmed - classification in Batch 4
BGP ORIGIN        : AS13335

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : APNIC Research and Development
NETWORK OPERATOR     : CLOUDFLARENET - Cloudflare, Inc.
RIR                  : APNIC
CONFIDENCE           : 98%

ASN intelligence
----------------
Routed prefix     : 1.1.1.0/24
Origin ASN(s)     : AS13335
Multi-origin      : no
AS13335           : CLOUDFLARENET - Cloudflare, Inc.
  Registry country: US
  ASN registry     : IANA 16-bit Autonomous System (AS) Numbers Registry

BGP route intelligence
----------------------
Observed origin   : AS13335
Origin consistent : yes
Routes observed   : 370
Unique AS paths   : 276
RIS collectors    : 23
Path-adjacent AS  : AS24482, AS199524, AS1299, AS8218, AS9002, AS34927, AS6461, AS49544
ASN neighbours    : 1537
```

IDEO-Lab

DEEP IP INTELLIGENCE ANALYZER



Metadata

Online

Version	0.3.0
Status	OK
Profile	quick
Target	1.1.1.1
Address family	IPv4
Category	public-global
Category detail	Public globally routable address
Globally routable	yes
Reverse pointer	1.1.1.1.in-addr.arpa
Duration	**1572.826 ms**

RDAP / RIR Registry

RIR	APNIC
IP range	1.1.1.0 - 1.1.1.255
CIDR	1.1.1.0 / 24
NetName	APNIC Research and Development
Registration	2011-08-10T23:12:35Z
Last update	2023-04-26T22:57:58Z
Status	active
Abuse contacts	IRT-APNICRANDNET-AU <helpdesk@apnic.net>

Network Ownership & Verdict

REGISTERED OWNER	APNIC Research and Development
ALLOCATED TO	APNIC Research and Development
CURRENT OPERATOR	CLOUDFLARENET – cloudflare, Inc.
HOSTING PROVIDER	unconfirmed - classification in Batch 4
BGP ORIGIN	AS13335

Verdict

INFRASTRUCTURE OWNER	APNIC Research and Development
NETWORK OPERATOR	CLOUDFLARENET - cloudflare, Inc.
RIR	APNIC
CONFIDENCE	**98%**



Analyzers

Unconfirmed
Specific RDAP in gelass analysis if paslt; routing analyzes correlate those signals later in the run.

ip-input	0.022 ms
rdap	363.927 ms

warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers correlate those signals later in the run.

asn	OK	726.051 ms
bgp	OK	395.641 ms
rpki	OK	87.137 ms

ASN & BGP intelligence

ASN intelligence

Routed prefix	1.1.1.0/24
Origin ASN(s)	AS13335
Multi-origin	no
AS13335	CLOUDFLARENET - cloudflare, Inc.
Registry country	US
ASN registry	IANA 16-bit Autonomous System (AS) Numbers Registry

BGP route intelligence

Observed origin	AS13335
Origin consistent	yes
Routes observed	**370**
Unique AS paths	**276**
RIS collectors	**23**
Path-adjacent AS	AS24482, AS199524, AS1299, AS8218, AS9002, AS34927, AS6461
ASN neighbours	**1537**

```
Target           : 2001:4860:4860::8888
Address family   : IPv6

ip-input          OK
rdap              OK
asn               OK
bgp               OK
rpki              OK
```

L'attribution IPv6 est également cohérente :

```
RIR              : ARIN
CIDR             : 2001:4860::/32
Organization     : Google LLC

CURRENT OPERATOR : GOOGLE - Google LLC
BGP ORIGIN       : AS15169
CONFIDENCE       : 98%
```

Et côté routage :

```
Routed prefix    : 2001:4860::/32
Origin ASN(s)    : AS15169
Multi-origin     : no

Observed origin  : AS15169
Origin consistent : yes
Routes observed  : 364
Unique AS paths  : 261
RIS collectors   : 23
ASN neighbours   : 332
```

IDEO-Lab

DEEP IP INTELLIGENCE ANALYZER



Metadata

Online

Version	0.3.0
Status	OK
Profile	quick
Target	2001:4860:4860::8888
Address family	IPv6
Category	public-global
Category detail	Public globally routable address
Globally routable	yes
Reverse pointer	[No reverse PTR found]
Duration	

RDAP / RIR Registry

RIR	ARIN
CIDR	2001:4860::/32
Organization	Google LLC
Registration	2011-08-10T23:12:35Z
Last update	2023-04-26T22:57:58Z
Status	active
Abuse contacts	<network-abuse@google.com>
Technical contacts	<arin-contact@google.com>

Network Ownership & Verdict

REGISTERED OWNER	Google LLC
ALLOCATED TO	Google LLC
CURRENT OPERATOR	GOOGLE - Google LLC
HOSTING PROVIDER	unconfirmed - classification in Batch 4
BGP ORIGIN	AS15169

Verdict & Confidence

INFRASTRUCTURE OWNER	Google LLC
NETWORK OPERATOR	GOOGLE - Google LLC
RIR	ARIN
CONFIDENCE	**98%**



Analyzers

warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers conselete those signals later in the run.

ip-input		0.022 ms
rdap		363.927 ms
asn	OK	OK
bgp	OK	OK
rpki	OK	OK

⚠ Current operator and BGP origin data unconfirmed until Batch 3

Analyses supplémentaires de routage recommandées.

ASN & BGP intelligence

ASN intelligence

Routed prefix	2001:4860::/32
Origin ASN(s)	AS15169
Multi-origin	no
Multi-origin list	no

BGP route intelligence

Observed origin	AS15169
Origin consistent	yes
Routes observed	**364**
Unique AS paths	**261**
RIS collectors	**23**
Path-adjacent AS	AS24482, AS199524, AS1299, AS8218, AS9002, AS34927, AS6461
ASN neighbours	**332**

IDEO-Lab

DEEP IP INTELLIGENCE ANALYZER



Metadata

Online

Version	0.3.0
Status	OK
Profile	quick
Target	2001:4860:4860::8888
Address family	IPv6
Category	public-global
Category detail	Public globally routable address
Globally routable	yes
Reverse pointer	[Full IPv6 reverse string from <IMAGE 1>, e.g. 8.8.8.8.0.0.0.0.0.0.0.0.0.0.0.0..0.0.0.6.8.4.0.6.8.4.1.0.0.2.ip6.arpa]
Duration	2433.475 ms

Analyzers

warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers conselete those signals later in the run.

ip-input	OK	0.043 ms
rdap	OK	684.472 ms
asn	OK	1007.437 ms
bgp	OK	472.187 ms
rpki	OK	269.278 ms

⚠ Current operator and BGP origin data unconfirmed until Batch 3

Analyses supplementaires de routage recommandées.

RDAP / RIR Registry

RIR	ARIN
IP range	2001:4860:: - 2001:4860:ffff:ffff:ffff:ffff:ffff
CIDR	2001:4860:: / 32
NetName	GOOGLE-IPv6
Organization	Google LLC
Registration	2005-03-14T11:31:08-05:00
Last update	2012-02-24T09:44:34-05:00
Status	active
Abuse contacts	<network-abuse@google.com>
Technical contacts	<arin-contact@google.com>

ASN & BGP intelligence

ASN intelligence	
Routed prefix	2001:4860::/32
Origin ASN(s)	AS15169
Multi-origin	no
AS15169	GOOGLE - Google LLC
Registry country	US
Registry	IANA 16-bit Autonomous System (AS) Numbers Registry

ASN & BGP intelligence

Registered Owner	Google LLC
Allocated To	Google LLC
Current Operator	GOOGLE - Google LLC
Hosting Provider	unconfirmed - classification in Batch 4
BGP Origin	AS15169

Verdict & Confidence

98%

BGP route intelligence

Observed origin	AS15169
Origin consistent	yes
Routes observed	**364**
Unique AS paths	**261**
RIS collectors	**23**
Path-adjacent AS	AS6939, AS24482, AS1299, AS214292, AS8218, AS9002, AS34019, AS6461
ASN neighbours	**332**

RPKI / routing security

RPKI verdict	VALID
AS15169	VALID (valid)

Batch 3 ASN/BGP/RPKI routing intelligence is ready. GEO intelligence arrives in Batch 4.

IDEO-Lab Deep IP Intelligence v0.3.0 • profile quick • 3171 ms

profile quick

8.8.8.8

OK

IPv4 • public-global • globally routable

PTR 8.8.8.8.in-addr.arpa.

ip-input	rdap	asn	bgp	rpki
OK	OK	OK	OK	OK

Ownership verdict

Google LLC

owner/operator

Confidence 98%

Hosting	unconfirmed Batch 4
BGP AS	AS15169

RDAP/RIR

Registry	ARIN
Handle	GOGL
CIDR	8.8.8.0/24
Organization	Google LLC
Status	active

Abuse contact

network-abuse@google.com

ASN intelligence

Prefix	8.8.8.0/24
ASN	AS15169
Multi-origin	No
Organization	GOOGLE Google LLC
Country	US
Registry / Type	IANA 16-bit

BGP route intelligence

Origin AS	AS15169 consistent
Routes (total)	374
Unique paths	283
RIS collectors	23
Neighbours	332

Path-adjacent ASes

AS3356 AS1299 AS6453 AS9002

BATCH 4



IP-INTEL-004 — Géolocalisation & type de réseau

Multi-source • Classification • Consensus.

004A Multi-Source Geolocation

chaque provider indépendant

Sources (providers indépendants)

A	Spain	Madrid
B	Spain	Madrid
C	Spain	Alcobendas
D	Spain	Madrid

Sources variées, qualité variable.
L'intelligence commence par la diversité.

004B Network Type Detection

classification chips

TYPES DE RÉSEAU DÉTECTÉS

Residential · Business · Hosting · Cloud · Datacenter

Mobile · VPN · Proxy · Tor · CDN

Anycast · University · Government · Satellite · Unknown

Classification multi-critères basée sur des signaux techniques et comportementaux.

004C Geo Consensus Engine

première vraie intelligence maison.

CONSENSUS GÉOGRAPHIQUE

Country	Spain	99%
Region	Madrid	91%
City	Madrid	72%
Estimated radius	35–80 km	

Consensus pondéré multi-sources.
Confiance maximale, transparence totale.

Ne jamais présenter une latitude comme une adresse exacte. | Toute géolocalisation est une estimation. Le consensus apporte la confiance, pas la certitude absolue.

IP-INTEL-004A — Multi-Source Geolocation

Abstraction permettant de comparer plusieurs bases.

Chaque provider sera indépendant.

Exemple :

```
SOURCE A     Spain    Madrid
SOURCE B     Spain    Madrid
SOURCE C     Spain    Alcobendas
SOURCE D     Spain    Madrid
```

IP-INTEL-004B — Network Type Detection

Classification :

```
Residential
Business
Hosting
Cloud
Datacenter
Mobile
VPN
Proxy
Tor
CDN
Anycast
University
Government
Satellite
Unknown
```

IP-INTEL-004C — Geo Consensus Engine

Première vraie intelligence maison.

Résultat :

```
COUNTRY
Spain
Confidence: 99%

REGION
Madrid
Confidence: 91%

CITY
Madrid
Confidence: 72%

ESTIMATED RADIUS
35-80 km
```

Le système devra refuser de présenter une latitude comme une adresse exacte.

```
Analyzers
---------
ip-input              OK
rdap                  OK
asn                   OK
bgp                   OK
rpki                  OK
geo                    OK
network-type           OK
geo-consensus          OK
```

Puis une nouvelle zone :

```
Geolocation sources
-------------------
ipwhois           : ...
ipapi             : ...
dbip              : ...
```

et :

```
Network type
------------
Primary type      : unknown / hosting / cloud / mobile / vpn / ...
Confidence        : ...
Candidates        : ...
```

```
Geo consensus
-------------
Country           : US United States | consensus 98%
Region            : California | consensus ...
City              : ... | consensus ...
Coordinates       : ...
Provider spread   : ... km
Estimated radius  : ... km [...]
Disagreements     : ...
Precision         : infrastructure-level only
```

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version           : 0.4.0
Status            : OK
Profile           : quick
Target            : 8.8.8.8
Address family    : IPv4
Category          : public-global
Category detail   : Public globally routable address
Globally routable : yes
Reverse pointer   : 8.8.8.8.in-addr.arpa
Duration          : 2694.149 ms

Analyzers
---------
ip-input             OK       0.021 ms
rdap                 OK       459.641 ms
  warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers correlate thos
e signals later in the run.
asn                  OK       685.641 ms
bgp                  OK       1271.732 ms
rpki                 OK       90.136 ms
geo                  OK       186.604 ms
network-type         OK       0.078 ms
  warning: No network type reached the minimum evidence threshold.
geo-consensus        OK       0.122 ms
  warning: Geolocation providers disagree on one or more location fields.

RDAP / RIR
----------
RIR               : ARIN
IP range          : 8.8.8.0 - 8.8.8.255
CIDR              : 8.8.8.0/24
NetName           : GOGL
Organization      : Google LLC
Registration      : 2023-12-28T17:24:33-05:00
Last update       : 2023-12-28T17:24:56-05:00
Status            : active
Abuse contacts    : Google Inc. <network-abuse@google.com>
Technical contacts: Google LLC <arin-contact@google.com>

Network ownership
-----------------
REGISTERED OWNER  : Google LLC
ALLOCATED TO      : Google LLC
CURRENT OPERATOR  : GOOGLE - Google LLC
HOSTING PROVIDER  : unconfirmed
BGP ORIGIN        : AS15169

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : Google LLC
NETWORK OPERATOR     : GOOGLE - Google LLC
RIR                  : ARIN
CONFIDENCE           : 98%

ASN intelligence
----------------
Routed prefix     : 8.8.8.0/24
Origin ASN(s)     : AS15169
Multi-origin      : no
AS15169           : GOOGLE - Google LLC
  Registry country: US
  ASN registry     : IANA 16-bit Autonomous System (AS) Numbers Registry

BGP route intelligence
```

```
BGP route intelligence
----------------------
Observed origin   : AS15169
Origin consistent : yes
Routes observed   : 374
Unique AS paths   : 283
RIS collectors    : 23
Path-adjacent AS  : AS214292, AS24482, AS8218, AS3356, AS9002, AS6453, AS1299, AS199524
ASN neighbours    : 332

RPKI / routing security
-----------------------
RPKI verdict      : VALID
AS15169           : VALID (valid)

Geolocation sources
-------------------
ipwhois           : San Jose, California, US
  coordinates      : 37.3393939, -121.8949553
ipapi             : Mountain View, California, US
  coordinates      : 37.42301, -122.083352
dbip              : Mountain View, California, US

Network type
------------
Primary type      : unknown
Confidence        : 0%

Geo consensus
-------------
Country           : US United States | consensus 98%
Region            : California | consensus 92%
City              : Mountain View | consensus 76%
Coordinates       : 37.38013, -121.986738
Provider spread   : 9.78 km
Estimated radius  : 100.0 km [provider-spread-heuristic]
Disagreements     : 1
Precision         : infrastructure-level only

Batch 4 multi-source GEO and network classification intelligence is ready. DNS/TLS intelligence arrives in
Batch 5.
```

```
CURRENT OPERATOR  : CLOUDFLARENET - Cloudflare, Inc.
BGP ORIGIN        : AS13335
CONFIDENCE        : 98%

Network type
------------
Primary type      : cdn
Confidence        : 98%
Candidates        : cdn=125
```

Et la partie GEO fait bien son travail de prudence :

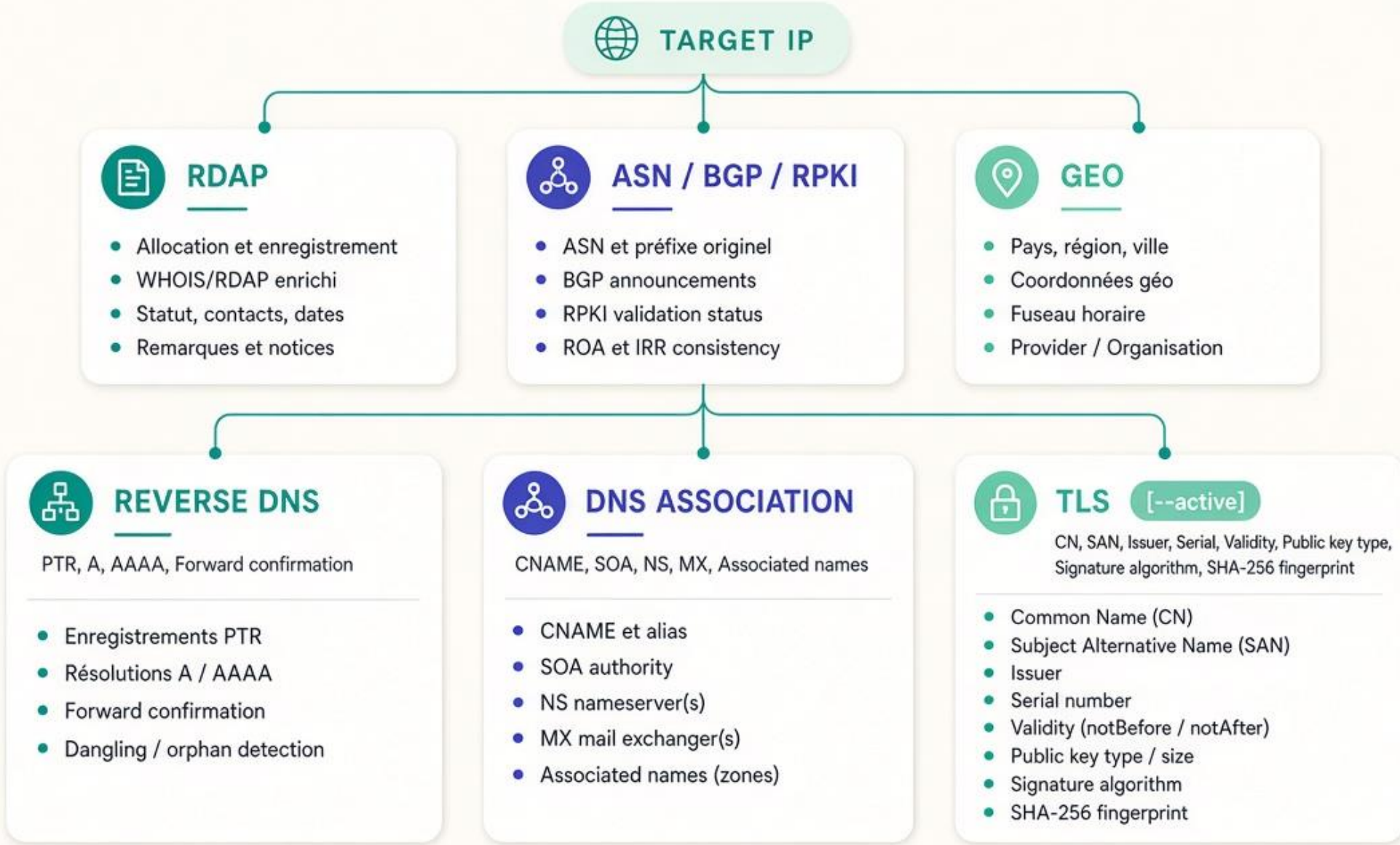
```
IPWhois : Brisbane, Queensland, AU
ipapi   : Sydney, New South Wales, AU
DB-IP   : Sydney, New South Wales, AU

Country           : AU Australia | consensus 98%
Region            : New South Wales | consensus 76%
City              : Sydney | consensus 70%
Provider spread   : 374.93 km
Estimated radius  : 562.4 km
Disagreements     : 3
```

BATCH 5



IP Intelligence — Arbre d'analyse

TARGET IP • sources passives et TLS actif



IP-INTEL-005A — Reverse DNS Analyzer

PTR + contrôle inverse :

```
IP → PTR
PTR → IP
```

Extraction éventuelle de codes POP/datacenter.

IP-INTEL-005B — DNS Association Analyzer

Recherche des associations :

```
A
AAAA
PTR
CNAME
MX
NS
domain associations
```

avec architecture prévue pour du passive DNS facultatif.

IP-INTEL-005C — TLS Certificate Intelligence

Analyse des certificats observables :

```
CN
SAN
Issuer
Serial
Fingerprint
Validity
Algorithm
Domains
```

Très utile pour relier plusieurs infrastructures entre elles.

IP-INTEL-005 — DNS Intelligence

Reverse DNS · Associations · Passive DNS facultatif

005A Reverse DNS Analyzer

PTR + contrôle inverse

IP → PTR → PTR (reverse DNS)

PTR → IP (forward)

Extraction éventuelle de codes POP / datacenter

Analyse et validation

- Résolution PTR réussie
- Correspondance forward confirmée
- Codes POP / datacenter détectés (si disponibles)
- Anomalies ou incohérences DNS

Vérification de confiance et d'intégrité reverse DNS

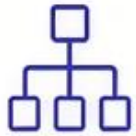
005B DNS Association Analyzer

Recherche des associations

Types d'enregistrements analysés

A | AAAA | PTR | CNAME | MX | NS | Domaines associés

Découverte des liens entre IP, noms d'hôtes et domaines



Associations directes et indirectes

Graphe de dépendances DNS

Enrichissement contextuel

Architecture prévue pour du Passive DNS facultatif

Passive DNS facultatif — enrichissement optionnel, pas un prérequis.

IP-INTEL — TLS certificate intelligence

Sonde active · certificat · identité

Handshake

Status
Handshake successful

SNI
example.com

Port
443

TLS version
TLS 1.3

Cipher
TLS_AES_256_GCM_SHA384

Certificate identity

CN
example.com

SAN DNS count
4

Associated domains
example.com · www.example.com · cdn.example.com · status.example.com

Issuer
Let's Encrypt Authority R3

Serial
03:ab:cd:12:34:56:78:90:ef:12:34:56:78:90:12:34:56

Crypto & validity

Valid from
2024-05-12 09:13:00 UTC

Valid until
2025-05-12 09:13:00 UTC

Key type
RSA 2048-bit

Signature
SHA256withRSA

SHA-256 fingerprint
ab:cd:ef:12:34:56:78:90:ab:cd:ef:12:34:56:78:90:
ab:cd:ef:12:34:56:78:90:ab:cd:ef:12:34:56

Module actif — connexion TLS réelle sur le port 443.

BATCH 6



IP-INTEL-006A — Passive Exposure Providers

Architecture pour exploiter facultativement :

Shodan, Censys ou autres sources équivalentes.

Le produit fonctionnera sans elles.

IP-INTEL-006B — Service Intelligence

Normalisation :

```
PORT
PROTOCOL
SERVICE
PRODUCT
VERSION
BANNER
FIRST SEEN
LAST SEEN
```

IP-INTEL-006C — Authorized Active Probe

Mode **explicitement optionnel** :

```bash
--active
```

destiné aux infrastructures que l'utilisateur possède ou est autorisé à tester.

Jamais lancé automatiquement.

Il pourra compléter les informations passives par des contrôles réseau légers et contrôlés.

IP-INTEL-006 — Exposition & services

Passif facultatif · Normalisation · Probe autorisé

006A Passive Exposure Providers

architecture facultative

Shodan | Censys | autres sources

Le produit fonctionne **SANS** elles.
Optional enrichment only.

006B Service Intelligence

Normalisation

PORT | PROTOCOL | SERVICE | PRODUCT
VERSION | BANNER | FIRST SEEN | LAST SEEN

Normalisation structurée des données pour une intégration et analyse fiables.

006C Authorized Active Probe

mode explicitement optionnel

`--active`

- infrastructures possédées ou autorisées uniquement.
- Jamais lancé automatiquement.
- Contrôles réseau légers et contrôlés.

Passif par défaut · Actif seulement avec `--active` et autorisation.

BATCH 7



IP-INTEL-007A — Reputation Provider Framework

Connecteurs optionnels pour :

VirusTotal, GreyNoise, AbuseIPDB et autres sources futures.

IP-INTEL-007B — Threat Evidence Correlator

Regroupement :

```
scanner
bot
brute force
spam
malware
C2
Tor
proxy
VPN
known benign crawler
```

avec timestamp obligatoire.

IP-INTEL-007C — IP Reputation Score

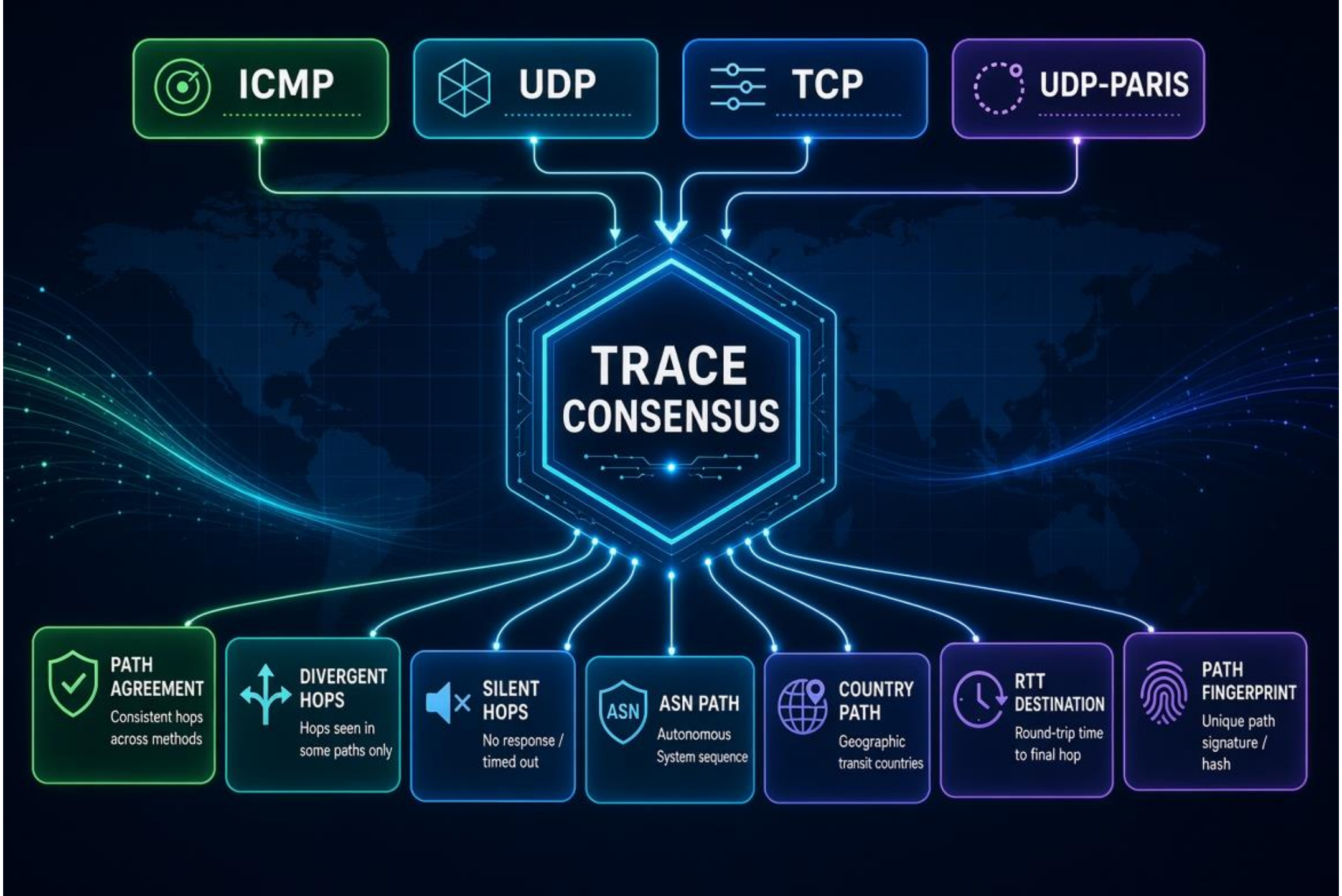
Création de notre propre résultat :

```
IP THREAT SCORE

18 / 100
LOW

Confidence: 87%
```

avec explication des éléments ayant fait évoluer le score.

BATCH 8




ICMP
UDP
TCP
UDP-PARIS
TRACE CONSENSUS
PATH AGREEMENT
Consistent hops across methods
DIVERGENT HOPS
Hops seen in some paths only
SILENT HOPS
No response / timed out
ASN
ASN PATH
Autonomous System sequence
COUNTRY PATH
Geographic transit countries
RTT DESTINATION
Round-trip time to final hop
PATH FINGERPRINT
Unique path signature / hash

IP-INTEL-008A — Native Trace Engine

Traceroute :

```
ICMP
UDP
TCP
```

avec timeout, retries et protection contre les routes interminables.

IP-INTEL-008B — Hop Intelligence

Chaque hop sera enrichi :

```
Hop 8
IP: xxx.xxx.xxx.xxx
ASN: ASxxxx
Operator: ...
Country: France
Probable POP: Paris
RTT: 18.7 ms
```

IP-INTEL-008C — Route Intelligence

Analyse de la route complète :

```
Home ISP
Transit
Internet Exchange
Backbone
Datacenter edge
Target
```

et détection des changements d'ASN.

IP-INTEL-008A — Native Trace Engine



timeout, retries and protection against endless routes

IP-INTEL-008C —

ROUTE INTELLIGENCE



COMPLETE ROUTE ANALYSIS AND ASN CHANGE DETECTION

BATCH 9



IP-INTEL-009C — Anycast & Geo Consistency

DETECTION INDICATORS

ANYCAST
IP shared across multiple locations

MULTIPLE POPs
Observed on multiple Points of Presence

CDN EDGE
Resolved via CDN edge infrastructure

ROUTE ASYMMETRY
Forward and return paths diverge

GEO DATABASE CONFLICT
GeoIP data conflicts with network behavior



SPECTACULAR EXAMPLE: GEO DB SAYS NEW YORK

GeoDB says
New York
United States



NETWORK OBSERVATIONS (RTT)
Latency from edge locations to the IP.

Madrid	8 ms	VERY SHORT
Paris	17 ms	SHORT
London	25 ms	SHORT
New York	92 ms	MODERATE / UNEXPECTED

NEW YORK LOCATION HIGHLY IMPROBABLE

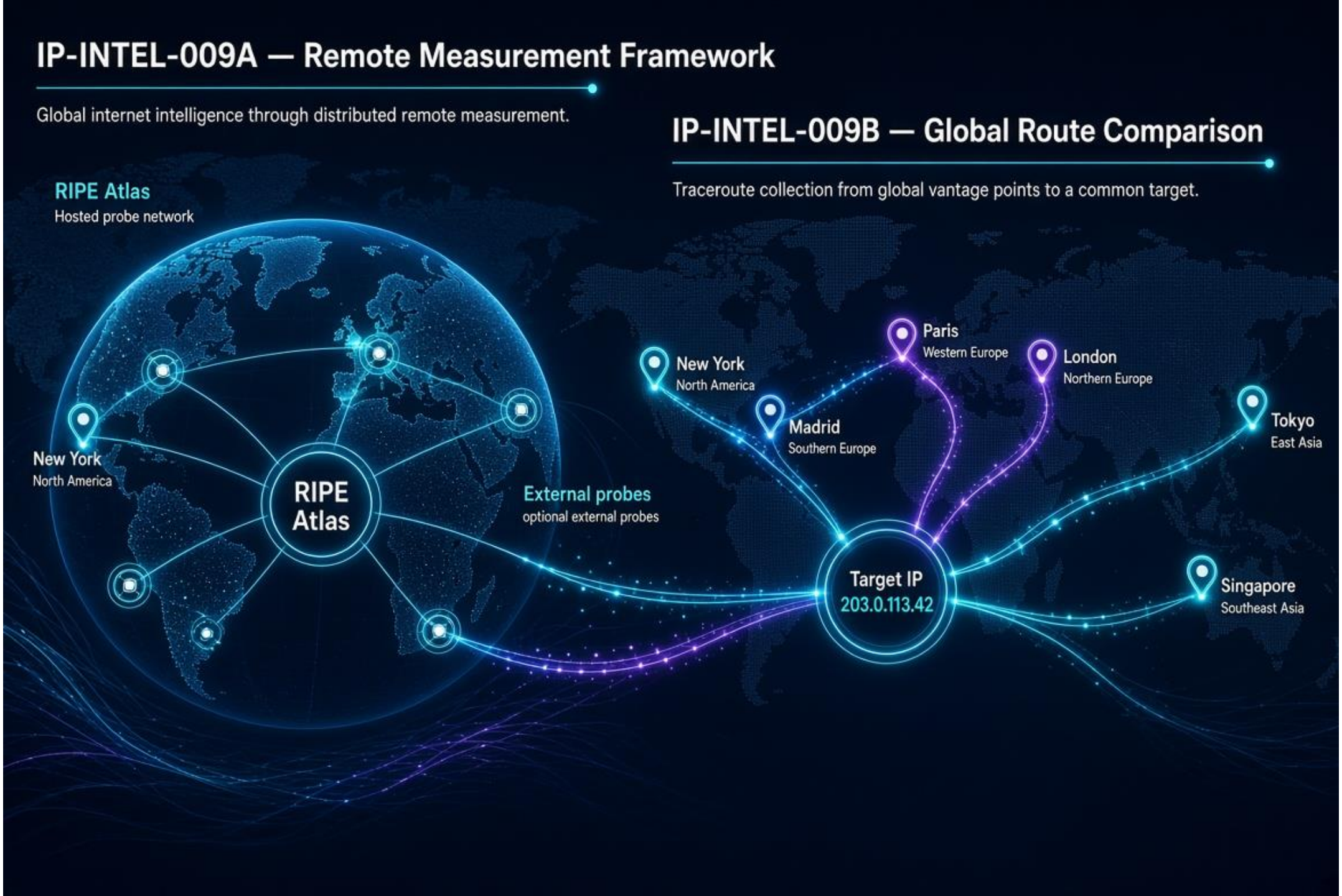
MULTIPLE INDICATORS SHOW GEO DATABASE CONFLICT AND NETWORK BEHAVIOR INCONSISTENCY

IP-INTEL-009A — Remote Measurement Framework

Global internet intelligence through distributed remote measurement.

IP-INTEL-009B — Global Route Comparison

Traceroute collection from global vantage points to a common target.



IP-INTEL-009A — Remote Measurement Framework

Support de probes externes facultatifs, par exemple RIPE Atlas.

IP-INTEL-009B — Global Route Comparison

Comparer :

```
Madrid
Paris
London
New York
Tokyo
Singapore
```

vers la même IP.

IP-INTEL-009C — Anycast & Geo Consistency

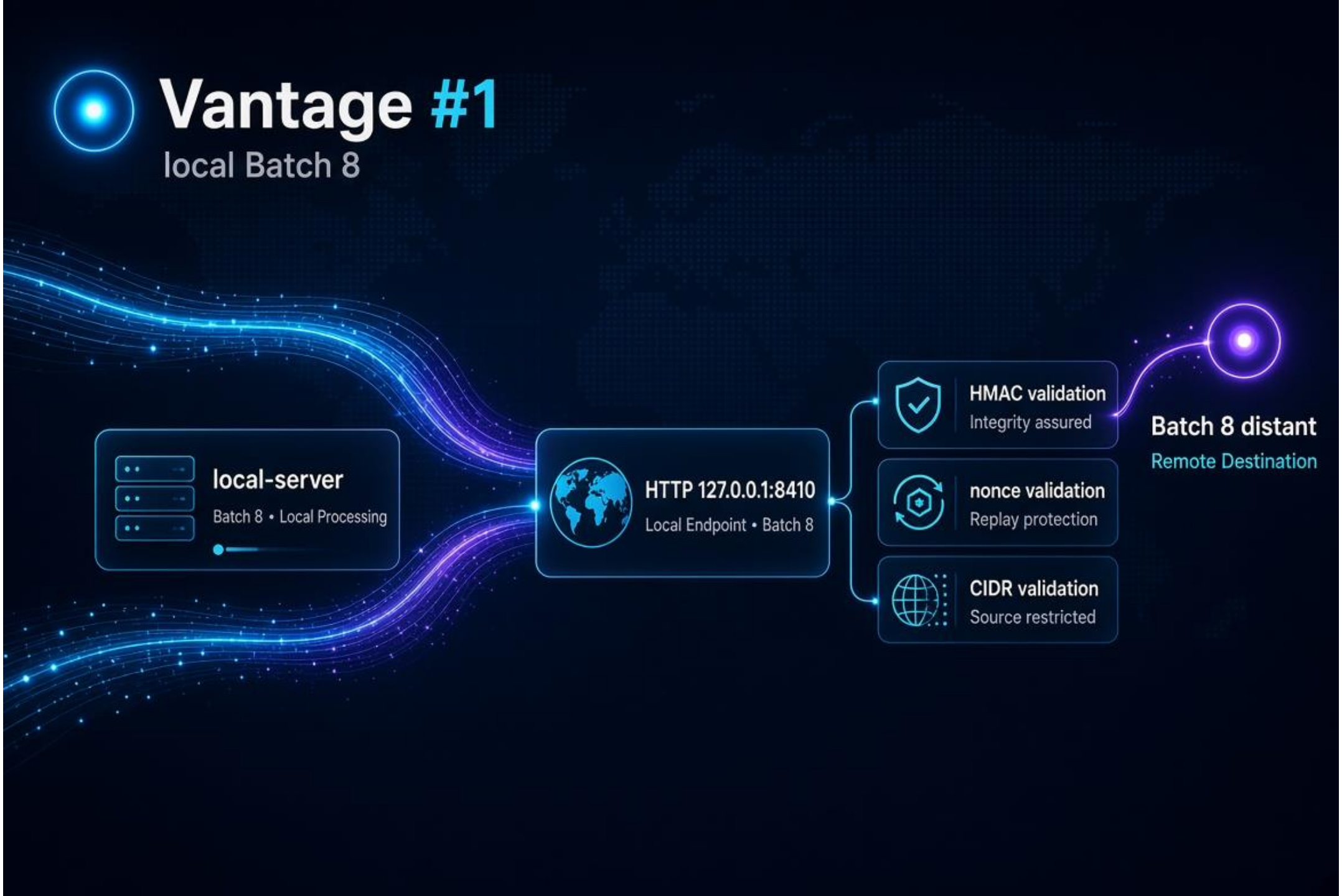
Détection possible de :

```
ANYCAST
MULTIPLE POPs
CDN EDGE
ROUTE ASYMMETRY
GEO DATABASE CONFLICT
```

Exemple spectaculaire :

```
GeoDB says: New York

Network observations:
Madrid RTT   8 ms
Paris RTT   17 ms
London RTT  25 ms
New York    92 ms

VERDICT:
New York location highly improbable.
```


TARGET IP
LOCAL ANALYZER
Frankfurt / AWS
Batch 8 trace
VANTAGE AGENT #1
Paris / Madrid
Batch 8 trace
VANTAGE AGENT #2
Warsaw / London
Batch 8 trace
MULTI-VANTAGE COLLECTOR
PATH DIVERSITY
Analyze alternate routes
RTT SPREAD
Measure latency variation
LATENCY GEOMETRY
Model network topology
MULTI-VANTAGE CONSENSUS
ASN DIVERSITY
Evaluate provider diversity
REACHABILITY
Validate end-to-end access
GEOGRAPHIC CONSTRAINTS
Assess regional factors


Vantage #1
local Batch 8
local-server
Batch 8 • Local Processing
HTTP 127.0.0.1:8410
Local Endpoint • Batch 8
HMAC validation
Integrity assured
nonce validation
Replay protection
CIDR validation
Source restricted
Batch 8 distant
Remote Destination

INTELLIGENCE PIPELINE

FROM SIGNAL TO SECURITY DECISION

THREAT INTELLIGENCE • INFRASTRUCTURE ANALYSIS • RISK REDUCTION



COLLECT → ENRICH → ANALYZE → CORRELATE → ACT

ACTIONABLE INTELLIGENCE. REDUCED RISK. STRONGER SECURITY.

BATCH 10



IP-INTEL-010A — Evidence Graph

Chaque information garde :

```
value
source
timestamp
confidence
reliability
```

IP-INTEL-010B — Conflict Detection

Détection automatique :

```
GeoIP conflict
ASN conflict
Owner conflict
DNS conflict
Historical conflict
Route conflict
```

Au lieu de choisir arbitrairement une valeur.

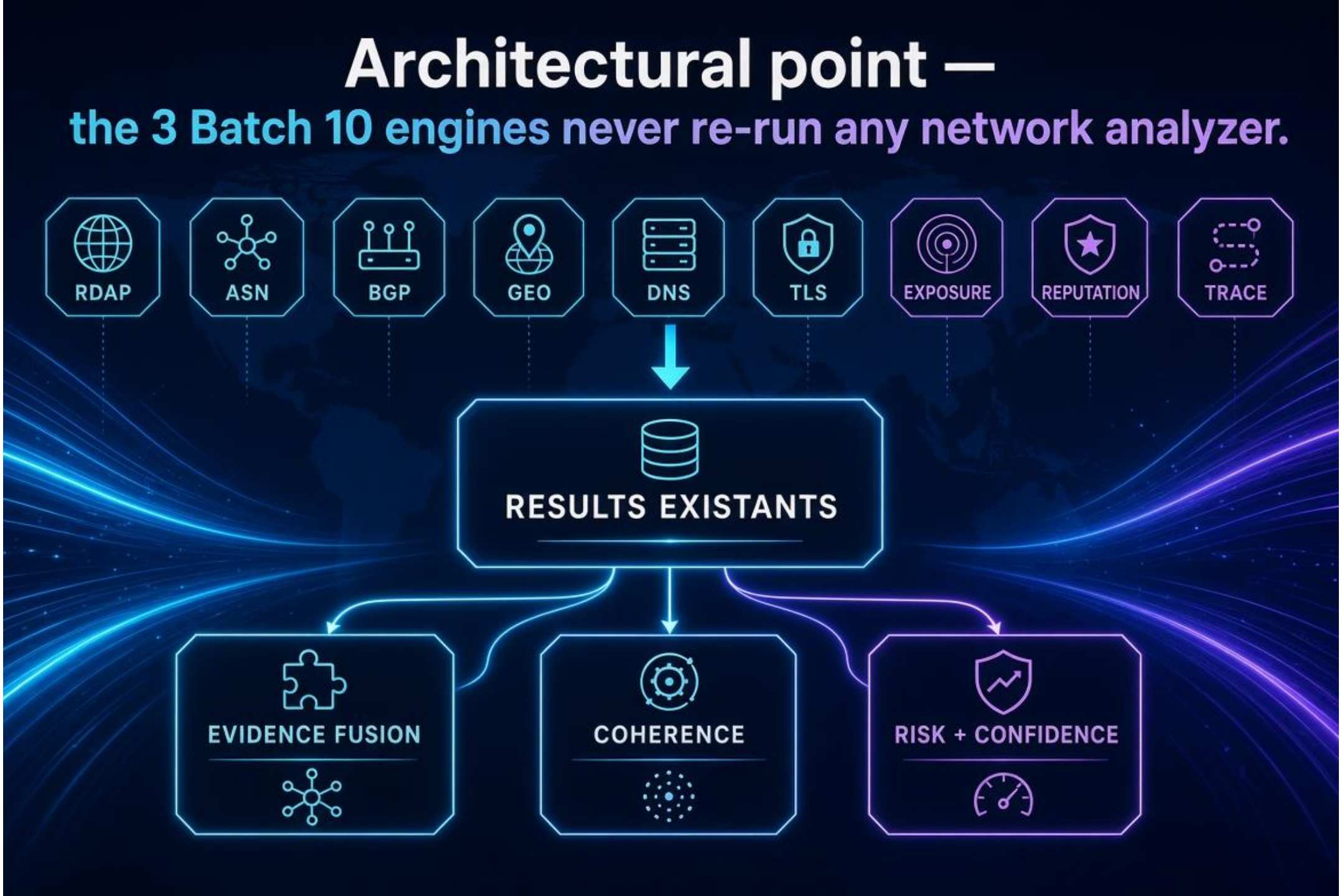
IP-INTEL-010C — Final Attribution Verdict

Production du grand résumé :

```
DEEP IP INTELLIGENCE VERDICT

Infrastructure Attribution: 96%
Country Attribution:        99%
Region Attribution:         89%
City Attribution:           62%
Hosting Classification:     97%
VPN Probability:            12%
Proxy Probability:           4%
Anycast Probability:         1%
Threat Score:               18/100
```

Architectural point —

the 3 Batch 10 engines never re-run any network analyzer.



BATCH 10 — CORRELATION ENGINE

IP-INTEL-010A
Evidence Fusion Core

Normalisation of existing results, evidence deduplication.

FAMILIES

- Identity
- Routing
- Geo
- DNS-TLS
- Exposure
- Reputation
- Trace

IP-INTEL-010B
Coherence & Contradiction Engine

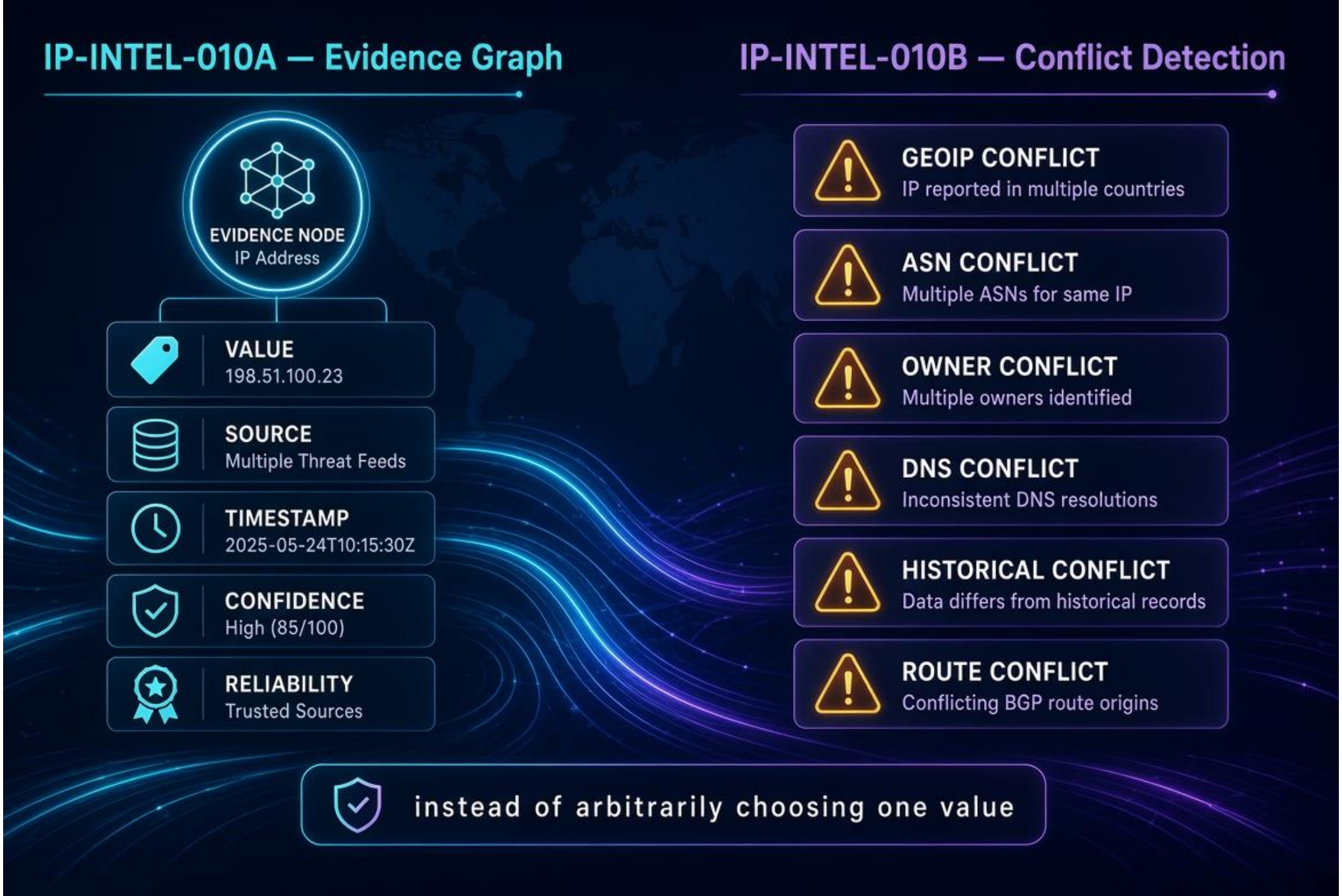
Paired analysis links for consistency, coverage, and contradiction detection.

ASN	⟷	BGP
BGP	⟷	RPKI
RDAP	⟷	operator
GEO	⟷	multi-source
PTR	⟷	forward DNS
DNS	⟷	TLS
Passive exposure	⟷	Active exposure
Reputation	⟷	infrastructure context
Trace ASN	⟷	destination ASN

IP-INTEL-010C
Confidence & Risk Synthesis

Confidence Score separate from Risk Score.

- **Confidence Score**
  Separate from Risk Score
- **Explanations**
  Full explanation of each point added/removed
- **Coverage**
  Depth, breadth, and gaps
- **Contradictions**
  Identified inconsistencies and impact
- **Evidence Quality**
  Source reliability and freshness
- **Limitations**
  Constraints and uncertainty
- **Final Technical Synthesis**
  Integrated conclusion and recommendations

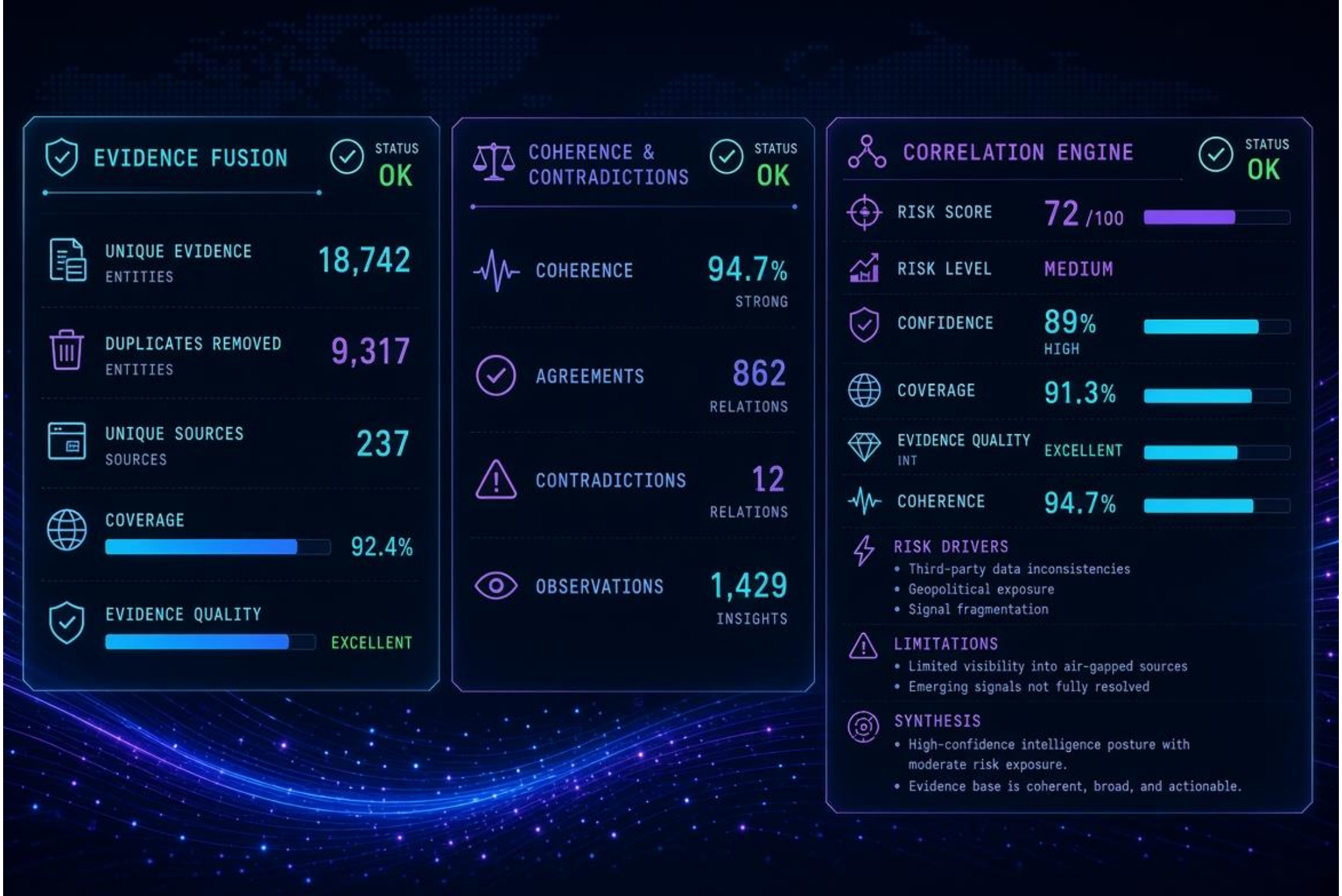

IP-INTEL-010A — Evidence Graph
EVIDENCE NODE
IP Address
VALUE
198.51.100.23
SOURCE
Multiple Threat Feeds
TIMESTAMP
2025-05-24T10:15:30Z
CONFIDENCE
High (85/100)
RELIABILITY
Trusted Sources
IP-INTEL-010B — Conflict Detection
GEOIP CONFLICT
IP reported in multiple countries
ASN CONFLICT
Multiple ASNs for same IP
OWNER CONFLICT
Multiple owners identified
DNS CONFLICT
Inconsistent DNS resolutions
HISTORICAL CONFLICT
Data differs from historical records
ROUTE CONFLICT
Conflicting BGP route origins
instead of arbitrarily choosing one value

IP-INTEL-010C — FINAL ATTRIBUTION VERDICT

DEEP IP INTELLIGENCE VERDICT

ATTRIBUTION & RISK ASSESSMENT SCOREBOARD

INFRASTRUCTURE ATTRIBUTION	96%
COUNTRY ATTRIBUTION	99%
REGION ATTRIBUTION	89%
CITY ATTRIBUTION	62%
HOSTING CLASSIFICATION	97%
VPN PROBABILITY	12%
PROXY PROBABILITY	4%
ANYCAST PROBABILITY	1%
THREAT SCORE	18/100


EVIDENCE FUSION
STATUS
OK
UNIQUE EVIDENCE
ENTITIES
18,742
DUPLICATES REMOVED
ENTITIES
9,317
UNIQUE SOURCES
SOURCES
237
COVERAGE
92.4%
EVIDENCE QUALITY
EXCELLENT
COHERENCE & CONTRADICTIONS
STATUS
OK
COHERENCE
94.7%
STRONG
AGREEMENTS
862
RELATIONS
CONTRADICTIONS
12
RELATIONS
OBSERVATIONS
1,429
INSIGHTS
CORRELATION ENGINE
STATUS
OK
RISK SCORE
72 /100
RISK LEVEL
MEDIUM
CONFIDENCE
89%
HIGH
COVERAGE
91.3%
EVIDENCE QUALITY
INT
EXCELLENT
COHERENCE
94.7%
RISK DRIVERS
• Third-party data inconsistencies
• Geopolitical exposure
• Signal fragmentation
LIMITATIONS
• Limited visibility into air-gapped sources
• Emerging signals not fully resolved
SYNTHESIS
• High-confidence intelligence posture with moderate risk exposure.
• Evidence base is coherent, broad, and actionable.

BATCH 10 — Heart of the system.



BATCH 10 — ÉTAT FINAL

VALIDATION TERMINÉE — PRÊT POUR DÉPLOIEMENT



IP-INTEL-010A

Evidence Fusion Core

VALIDÉ

IP-INTEL-010B

Coherence & Contradiction Engine

VALIDÉ

IP-INTEL-010C

Confidence & Risk Synthesis

VALIDÉ

VÉRIFICATIONS D'INTÉGRITÉ

- Evidence deduplication
- Family coverage
- Source quality
- Cross-source agreements
- Contradictions
- Context observations

VÉRIFICATIONS SÉMANTIQUES & QUALITÉ

- Risk Score
- Confidence Score
- Risk ≠ Confidence
- Explainability
- Limitations
- Standalone / no new dependency

BATCH 11



SCAN INTELLIGENCE PIPELINE

FROM DISCOVERY TO ACTIONABLE INTELLIGENCE



CONTINUOUS INTELLIGENCE • ACTIONABLE INSIGHT • REDUCED RISK

IP-INTEL-011A — Historical Network State

Historique :

```
ASN
prefix
owner
BGP
```

IP-INTEL-011B — Historical DNS / TLS / Services

Lorsqu'une source le permet :

```
domains
certificates
services
hostnames
```

avec `FIRST SEEN / LAST SEEN`.

IP-INTEL-011C — IP Timeline

Vue :

```
2022 ——— 2023 ——— 2024 ——— 2025 ——— 2026
   ASN A       ASN A       ASN B       ASN B       ASN C
```

Ce que le premier scan donnera — Historical Intelligence

CYBER THREAT INTELLIGENCE

1 FIRST SCAN / BASELINE

Establishing the initial security posture

OK

Mode	baseline
Snapshots	1
Snapshot ID	1
Previous ID	—
Material changes	0
Coverage changes	0
Highest severity	none
Risk delta	baseline
Confidence delta	baseline
Risk trend	baseline

Risk trend
baseline

2 SECOND SCAN SAME IP NO CHANGE

No detected differences from baseline

UNCHANGED

Mode	unchanged
Snapshots	2
Previous ID	1
Material changes	0
Risk delta	0.0
Confidence delta	0.0
Risk trend	stable

Risk trend
stable

3 IF BGP CHANGES

Routing or path changes detected

CHANGED

Mode	changed
Snapshots	2
Previous ID	1
Material changes	1
Coverage changes	1
Highest severity	high
Changed sections	routing
Risk delta	+2.7
Confidence delta	-15.0%
Risk trend	increasing

Risk trend
increasing

HISTORICAL INTELLIGENCE • CONTINUOUS VALIDATION • RISK-AWARE SECURITY

BATCH 12

IP-INTEL-012C

— INVESTOR-GRADE VISUALIZATION

Institutional-grade intelligence. Verified. Contextual. Actionable.

VISUALIZATION SHOWCASE

- OVERVIEW
- GEO
- OWNERSHIP
- ASN/BGP
- TRACE
- DNS
- TLS
- SERVICES
- THREATS
- HISTORY
- EDDENCE
- EVIDENCE

INVESTOR-GRADE INTELLIGENCE
TRANSPARENT | VERIFIED | RELIABLE

GEO DISTRIBUTION



United States	42%
Germany	23%
Singapore	14%
Netherlands	8%
Other	13%

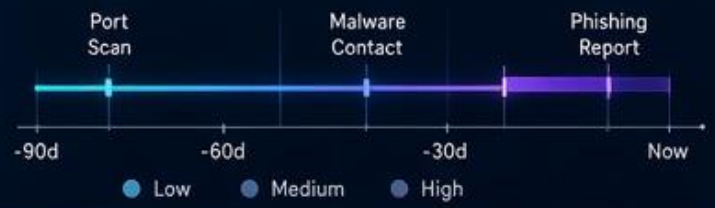
RISK & CONFIDENCE GAUGE



STRONG

Data Quality • Cross-Validated

THREAT TIMELINE



ASN / BGP GRAPH



4 Direct Peers • 12 Announced Prefixes

TRACEROUTE VISUALIZATION



CONFIDENCE BADGE

HIGH CONFIDENCE
87 / 100

- Multi-source validation
- Low volatility
- No conflicts

VISIBLE CONTRADICTIONS

TLS CERT MISMATCH
Certificate CN: *.example.com
Observed Host: 104.21.35.45

CONTRADICTION DETECTED

MINI-MODAL EXPLANATION

WHY THIS MATTERS

This IP belongs to a network with elevated risk indicators and visible inconsistencies.

INVESTOR IMPLICATION

Increased scrutiny recommended. Verify control, ownership, and operational risk before capital allocation.

All data verified from multiple independent sources. Last updated: 2025-05-21 10:24 UTC

IP-INTEL-012A Dashboard Bridge

Dashboard calls dedicated analysis engine.

DASHBOARD

IP INTELLIGENCE DASHBOARD

Centralized interface for IP intelligence operations.

CALLS

Sends IP and parameters to the analysis engine.

IP_ANALYZER ENGINE

IP_ANALYZER

Dedicated intelligence engine. Performs deep analysis, enrichment, and threat modeling.

CLI STILL WORKS INDEPENDENTLY.

IP_ANALYZER can be used directly via command line outside the dashboard.

DEEP IP INTELLIGENCE

Advanced IP intelligence workspace

ENTER IP ADDRESS

e.g., 203.0.113.45

SELECT ANALYSIS MODE

QUICK
Fast reputation and risk check

DEEP
In-depth behavioral and contextual analysis

FORENSIC TRACE
Trace infrastructure, relations and attack paths

ANALYZE IP

INTELLIGENT IP ANALYTICS. PRECISE. ACTIONABLE. SECURE.

IP-INTEL-012A — Dashboard Bridge

Le dashboard pourra appeler :

```
IP_ANALYZER
```

comme un moteur séparé.

Le CLI continuera de fonctionner indépendamment.

IP-INTEL-012B — Deep IP Intelligence Workspace

Nouvelle interface :

```
┌──────────────────────────────────────────────┐
│           DEEP IP INTELLIGENCE               │
│                                              │
│ IP: [_____________________________]          │
│                                              │
│ QUICK   DEEP   FORENSIC TRACE                │
│                                              │
│              ANALYZE IP                      │
└──────────────────────────────────────────────┘
```

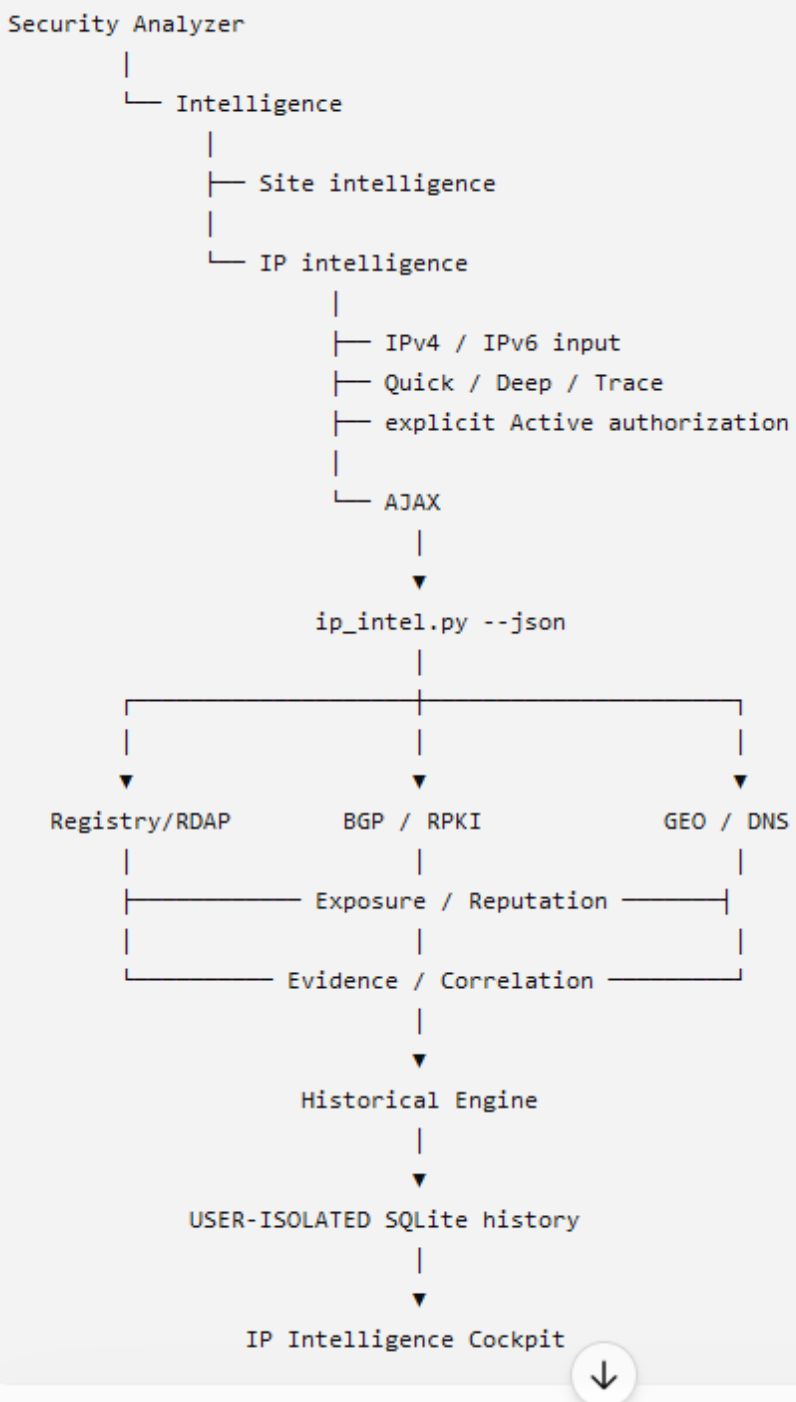
IP-INTEL-012C — Investor-Grade Visualization

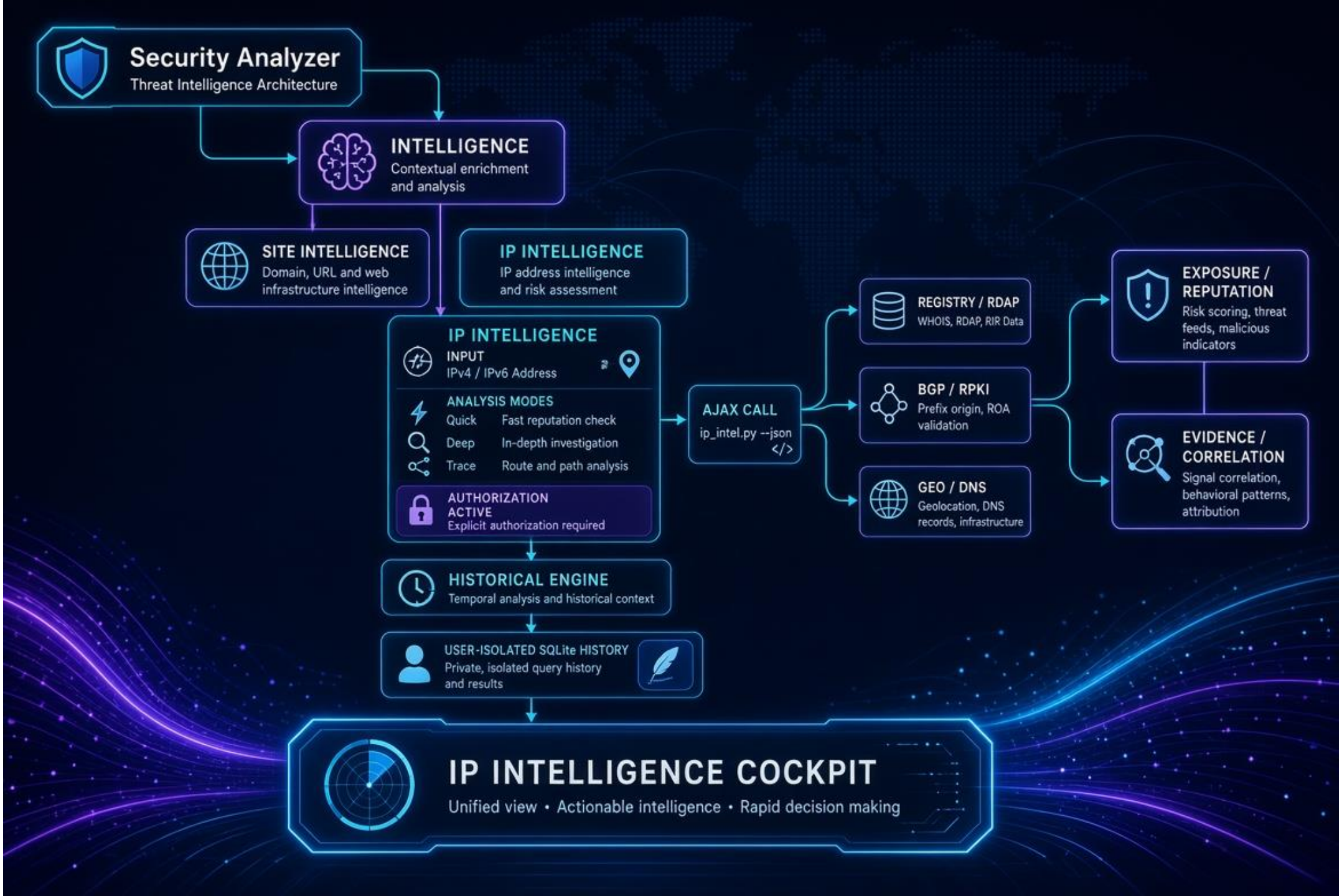
Et là nous faisons quelque chose de beaucoup plus spectaculaire :

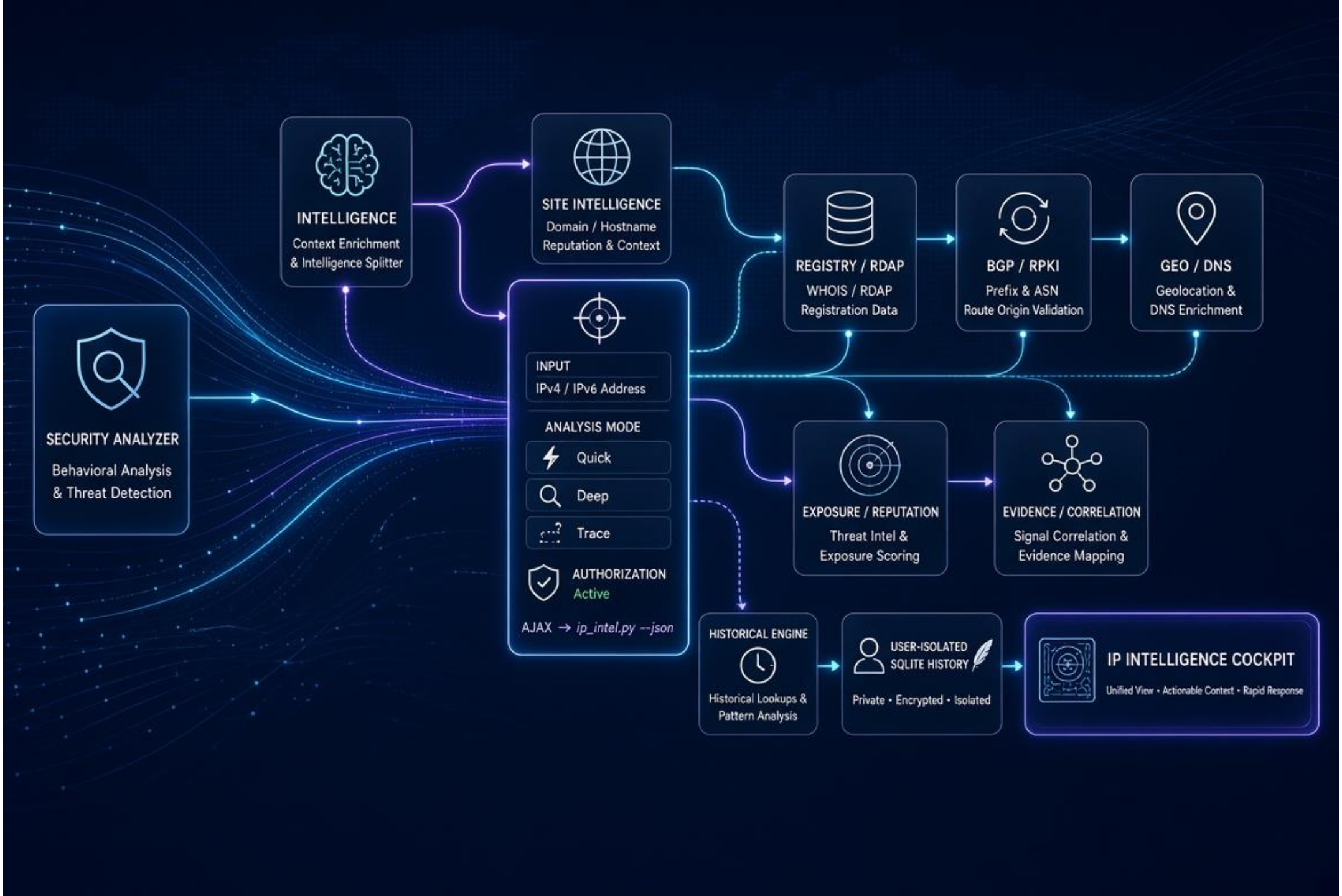
```
OVERVIEW
GEO
OWNERSHIP
ASN/BGP
TRACE
DNS
TLS
SERVICES
THREATS
HISTORY
EVIDENCE
```

avec :

- cartes ;
- jauges ;
- timeline ;
- graphe ASN ;
- représentation du traceroute ;
- badges de confiance ;
- contradictions visibles ;
- explications par mini-modals.


Security Analyzer
Intelligence
Site intelligence
IP intelligence
IPv4 / IPv6 input
Quick / Deep / Trace
explicit Active authorization
AJAX
ip_intel.py --json
Registry/RDAP
BGP / RPKI
GEO / DNS
Exposure / Reputation
Evidence / Correlation
Historical Engine
USER-ISOLATED SQLite history
IP Intelligence Cockpit


Security Analyzer
Threat Intelligence Architecture
INTELLIGENCE
Contextual enrichment and analysis
SITE INTELLIGENCE
Domain, URL and web infrastructure intelligence
IP INTELLIGENCE
IP address intelligence and risk assessment
IP INTELLIGENCE
INPUT
IPv4 / IPv6 Address
ANALYSIS MODES
Quick Fast reputation check
Deep In-depth investigation
Trace Route and path analysis
AUTHORIZATION ACTIVE
Explicit authorization required
AJAX CALL
ip_intel.py --json
REGISTRY / RDAP
WHOIS, RDAP, RIR Data
BGP / RPKI
Prefix origin, ROA validation
GEO / DNS
Geolocation, DNS records, infrastructure
EXPOSURE / REPUTATION
Risk scoring, threat feeds, malicious indicators
EVIDENCE / CORRELATION
Signal correlation, behavioral patterns, attribution
HISTORICAL ENGINE
Temporal analysis and historical context
USER-ISOLATED SQLite HISTORY
Private, isolated query history and results
IP INTELLIGENCE COCKPIT
Unified view • Actionable intelligence • Rapid decision making


INTELLIGENCE
Context Enrichment & Intelligence Splitter
SITE INTELLIGENCE
Domain / Hostname Reputation & Context
REGISTRY / RDAP
WHOIS / RDAP Registration Data
BGP / RPKI
Prefix & ASN Route Origin Validation
GEO / DNS
Geolocation & DNS Enrichment
SECURITY ANALYZER
Behavioral Analysis & Threat Detection
INPUT
IPv4 / IPv6 Address
ANALYSIS MODE
Quick
Deep
Trace
AUTHORIZATION
Active
AJAX → ip_intel.py --json
EXPOSURE / REPUTATION
Threat Intel & Exposure Scoring
EVIDENCE / CORRELATION
Signal Correlation & Evidence Mapping
HISTORICAL ENGINE
Historical Lookups & Pattern Analysis
USER-ISOLATED SQLITE HISTORY
Private • Encrypted • Isolated
IP INTELLIGENCE COCKPIT
Unified View • Actionable Context • Rapid Response

IP-INTEL-012A

Refaire complètement la page Overview pour coller au mockup

- structure beaucoup plus lisible
- hiérarchie visuelle forte
- cartes utiles
- suppression de l'effet "tableau de blocs des années 90"
- vue synthétique **investor-grade**

IP-INTEL-012B

Rendre la zone Evidence records exploitable

- accès via **onglet horizontal**
- **filtres**
- **search**
- **pagination**

IP-INTEL-012C

Rendre la zone Analyzer execution exploitable

- accès via **onglet horizontal**
- **filtres**
- **search**
- **tri**
- **pagination**

3) STRATÉGIE DE MODIFICATION

Je te propose de ne **pas faire un bricolage local**, mais au contraire de faire un **vrai refactoring visuel ciblé** du dashboard IP.

Le bon périmètre est :

- remplacement de la fonction `_render_overview(...)`
- refonte de la fonction `_render_evidence(...)`
- enrichissement du helper `_table(...)` en un vrai composant "data explorer"
- extension du **CSS** embarqué
- extension du **JavaScript** embarqué

Règles de mapping de données

Geo distribution

À calculer à partir de `raw_geo.get("sources")` :

- compter les pays vus chez les providers
- calculer % par fréquence
- afficher top 5

Risk & confidence gauge

Utiliser :

- `correlation["confidence_percent"]`
- `correlation["confidence_level"]`
- `correlation["risk_level"]`
- `correlation["risk_score"]`

Observation timeline

Utiliser :

- `history["first_seen"]`
- `history["previous_seen"]`
- `history["snapshot_count"]`
- `history["mode"]`

⚠️ On **n'invente pas de faux événements.**
On stylise une timeline à partir des jalons réellement disponibles.

ASN / BGP graph summary

Utiliser :

- `asn["origin_asns"]`
- `bgp["path_adjacent_asns"]`
- `bgp["route_count"]`
- `bgp["unique_as_paths"]`

Traceroute visualization

Utiliser :

- `trace-consensus`
- `trace-hops`
- sinon fallback propre "No active trace path available"

Confidence badge

Utiliser :

- confidence %
- agreements
- contradictions
- evidence quality

A.2 — Ajouter des helpers de rendu overview

À insérer juste après `_panel(...)`

Juste après la fonction `_panel(...)` (qui commence ligne 461),

ajouter ces nouveaux helpers :

- `_overview_country_distribution(raw_geo)`
- `_overview_timeline(history)`
- `_overview_asn_summary(asn, bgp)`
- `_overview_trace_summary(trace_consensus, trace_hops)`
- `_overview_confidence_badge(correlation, coherence, fusion)`
- `_overview_investor_implication(correlation, coherence)`

👉 Objectif : **éviter un `_render_overview()` monstrueux**.

Evidence records

Doit être déplacé dans le sous-onglet **Evidence records**
et rendu via un nouveau composant “explorer table” :

fonctionnalités minimales obligatoires

- **search**
- **filters**
  - Family
  - Analyzer
  - Type
- **pagination**
- compteur du nombre de lignes visibles

comportement UX

- 10 lignes par page par défaut
- options : 10 / 25 / 50
- message vide propre si aucun résultat
- filtre/search côté client en JS

nouveau helper recommandé

- `_simple_table(...)` pour les tableaux simples
- `_explorer_table(...)` pour les listes filtrables/paginées

`_explorer_table(...)` doit accepter au minimum

- `table_id`
- `headers`
- `rows`
- `empty_message`
- `filter_specs`
- `sortable`
- `page_size`

Exemple de `filter_specs` pour **Evidence records** :

- `family`
- `analyzer`
- `type`

B.3 — Données Evidence records

Les colonnes restent :

- Family
- Analyzer
- Source
- Type
- Confidence

Mais elles doivent être émises avec des attributs `data-*` sur chaque ligne, par exemple :

- `data-family`
- `data-analyzer`
- `data-type`

pour permettre les filtres côté JS.

Fonctions obligatoires

- **search**
- **filter**
  - status
  - analyzer
- **sort**
  - analyzer
  - status
  - duration
- **pagination**

Colonnes

- Analyzer
- Status
- Duration
- Warnings

Règles de tri

- tri par défaut : **duration desc**
- tri cliquable sur les en-têtes

1. onglets principaux

Déjà existants :

- Overview
- Geo
- Ownership
- ASN/BGP
- Trace
- DNS/TLS
- Services
- Threats
- History
- Evidence

2. sous-onglets internes Evidence

Nouveaux :

- Summary
- Evidence records
- Analyzer execution

3. explorers de table

Pour chaque explorer :

- lecture des lignes
- filtre par select
- search text
- tri colonnes
- pagination
- compteur “showing X of Y”

Overview

On doit avoir une page :

- beaucoup plus belle
- beaucoup plus structurée
- beaucoup plus “cockpit”
- bien plus proche du mockup

et surtout :

- **moins de grosses tables**
- plus de **cards synthétiques**
- un **rendu investisseur / démo**

Evidence

On doit avoir :

- un onglet **Summary**
- un onglet **Evidence records**
- un onglet **Analyzer execution**

et les deux listes deviennent enfin **utilisables.**

Structure cible — IP Intelligence Cockpit

Live • Updated just now

Analysed target IP
203.0.113.42 IPv4

Profile
Infrastructure • Hosting • APAC

Duration
30 days
(2025-04-21 – 2025-05-21)

Confidence
HIGH 87/100

Risk score
72 /100
Elevated Risk
Driven by threats, contradictions and exposure

Confidence
87 /100
High Confidence
Strong evidence density and consistency

Coherence
81 /100
Mostly Coherent
Minor gaps in alignment and attribution

Evidence quality
88 /100
High Quality
Reliable sources with strong signal strength

Geo distribution
Observed IP presence and activity



- Primary 42%
- Secondary 28%
- Tertiary 18%
- Other 12%

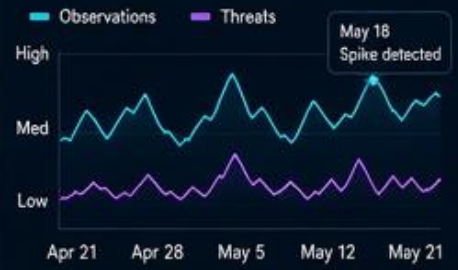
Top regions: APAC • Europe • North America

Risk & confidence gauge
Current posture snapshot



Risk	Confidence
72 /100	87 /100

Observation / threat timeline
Events and threats over analysis window



ASN / BGP graph summary
Top ASNs by observed activity



AS17621	CHINANET-BACKBONE	38%
AS45102	CNNIC-ALIBABA-CN-NET	22%
AS24940	HETZNER-AS	14%
AS16509	AMAZON-02	9%
AS53667	WHG-USA	6%

View full BGP graph →

Traceroute visualization
Reconstructed routing path



203.0.113.1	203.0.113.42	198.51.100.10	198.51.100.14	203.0.113.42
Your Edge	Target IP	AS17621	AS45102	Target IP
2 ms	6 ms	18 ms	34 ms	46 ms

Confidence badge
IP intelligence confidence level



Strong evidence density, reliable sources, and consistent behaviour support high confidence in this assessment.

0 0
LOW MEDIUM HIGH

Visible contradictions
Potential inconsistencies and red flags

Moderate contradictions detected
Observed data conflicts reduce attribution certainty.

- IP seen in both hosting and residential ranges
- Conflicting geolocation signals (CN ↔ SG)
- Unusual BGP path changes during window

Review contradictions →

Mini explanation / investor implication
Key takeaway for decision makers

Why this IP matters
Infrastructure IP with elevated risk and strong confidence. Linked to active hosting infrastructure in APAC with observed threats and routing anomalies.

Investor implication
Increased attack surface risk. Factor into due diligence, exposure scoring, and vendor / infrastructure risk decisions.

BATCH 12
GEO IP


OVERVIEW
GEO DISTRIBUTION
United States
100%
EXPAND
GEO DISTRIBUTION — GOOGLE MAPS
Map
Satellite
Street View
Fullscreen
San Francisco
Oakland
San Jose
Mountain View
COUNTRY CONSENSUS
United States
100%
PROVIDERS
ipwhois
San Jose, CA
37.XX, -121.XX
ipapi
Mountain View, CA
37.XX, -122.XX

GEO LOCATION

EXPAND



3.72.171.177

Frankfurt am Main

Hesse · Germany

Confidence
98%

Radius
≈100 km

IP LOCATION — 3.72.171.177



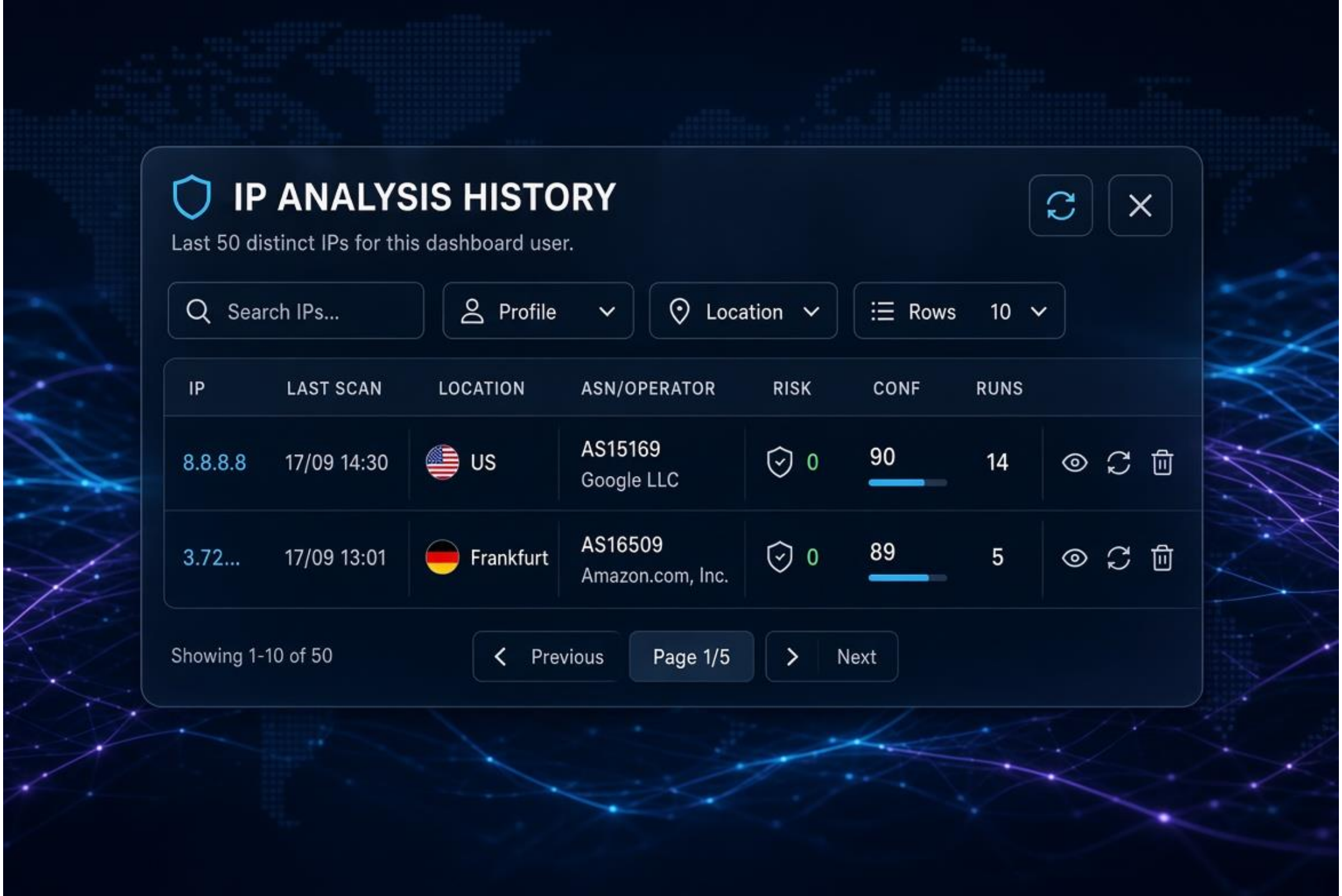
ESTIMATED LOCATION
Frankfurt am Main
Hesse
Germany

CONSENSUS
50.109179, 8.657732

RADIUS
≈100 km

SPREAD
2.12 km


IP INTELLIGENCE
RUN NEW ANALYSIS
SCAN HISTORY
LAST 50 DISTINCT IPs
Filter IPs...
Sort: Recent
All
8.8.8.8
15 runs
3.72.171.177
4 runs
1.1.1.1
2 runs
1 – 3 of 50
1
2
3
....
17
Show 3 per page
CLICK IP / RUNS
HISTORY OF THIS IP


IP ANALYSIS HISTORY
Last 50 distinct IPs for this dashboard user.
Search IPs...
Profile
Location
Rows 10
IP
LAST SCAN
LOCATION
ASN/OPERATOR
RISK
CONF
RUNS
8.8.8.8
17/09 14:30
US
AS15169
Google LLC
0
90
14
3.72...
17/09 13:01
Frankfurt
AS16509
Amazon.com, Inc.
0
89
5
Showing 1-10 of 50
Previous
Page 1/5
Next

CYBERSECURITY ARCHITECTURE FLOW

IP INTELLIGENCE NAVIGATION PIPELINE



SECURE • CLEAN • CONTEXT-PRESERVING • INVESTOR-GRADE

INTELLIGENT NAVIGATION PIPELINE ENFORCES SECURITY AND DELIVERS PRECISE STATE

BATCH 12 DASHBOARD

```
Coherence & contradictions
--------------------------
Status             : OK
Coherence          : 96%
Agreements         : 4
Contradictions     : 1
Observations       : 4
  CONTRADICTION [MEDIUM] GEO_PROVIDER_DISAGREEMENT
    Geolocation consensus reports 1 disagreement(s).
  OBSERVATION PTR_FORWARD_MISMATCH - Reverse DNS does not forward-confirm
  OBSERVATION DNS_TLS_NAME_DIVERGENCE - DNS and TLS names differ
  OBSERVATION REPUTATION_LOW_COVERAGE - Reputation coverage is limited
  OBSERVATION NETWORK_TYPE_UNRESOLVED - Network type remains unresolved

Correlation Engine
------------------
Status             : OK
Risk score         : 0/100
Risk level         : LOW-OBSERVED-RISK
Confidence         : 89.5%
Confidence level   : HIGH
Coverage           : 90.0%
Evidence quality   : 85.2%
Coherence          : 96.0%
Risk drivers       : 0
Limitations        : 4
  - No evaluable trace core evidence is available in this profile.
  - Reputation coverage is limited to 25.0% of the configured provider set.
  - PTR forward-confirmation is incomplete; split-horizon or provider-internal DNS may explain the mis
match.
  - DNS-derived names and certificate names differ; virtual hosting or CDN behavior can make this legi
timate.
Synthesis          :
  - BGP origin is consistent with ASN routing intelligence.
  - RPKI validation is valid for the observed origin/prefix combination.
  - Geolocation converges on DE with 98% country-level consensus.
  - Reputation consensus reports 0/100 risk with 45% provider confidence.
  - No material adverse technical driver was observed in the currently available evidence.
  - 1 cross-source contradiction(s) remain visible in the synthesis.
Interpretation     : Risk measures adverse technical signals. Confidence measures how strongly the avai
lable evidence supports the synthesis. A low risk score is not a guarantee that the target is safe.

Historical Intelligence
-----------------------
Status             : OK
Mode               : unchanged
Snapshots          : 2
Snapshot ID        : 4
Previous ID        : 3
First seen         : 2026-09-17T13:25:28.089838+00:00
Previous seen      : 2026-09-17T13:25:28.089838+00:00
Material changes   : 0
Coverage changes   : 0
Highest severity   : none
Risk delta         : 0.0
Confidence delta   : 0.0
Risk trend         : stable
Confidence trend   : stable
Changed sections   : -

Run warnings
------------
- Active mode enabled. Existing active analyzers may run. Batch 11 historical intelligence is passive
and stores compact local snapshots after correlation.
```

```
Service exposure
----------------
Status            : OK
Observed services : 2
Review priority   : HIGH=0, REVIEW=0, NORMAL=2
     80  http             web            priority=normal
    443  https            web            priority=normal
Products          : f5/nginx

Active exposure validation
--------------------------
Status            : OK
Probe scope       : tcp-connect-only
Open TCP          : 80, 443
Closed TCP        : -
Indeterminate     : 21, 22, 25, 53, 110, 143, 445, 587, 993, 995, 3306, 3389, 5432, 8080
Passive confirmed : 80, 443
Newly observed    : -
Passive not now   : -

Reputation sources
------------------
Status            : OK
GreyNoise Community : not-found | RIOT=no | noise=no
AbuseIPDB           : not-configured
ThreatFox           : not-configured
Spamhaus ZEN        : not-configured

Abuse signals
-------------
Status            : OK
Providers evaluated: 1
Adverse signals   : 0
Reassuring signals: 0
Context signals   : 0

Reputation consensus
--------------------
Status            : OK
Verdict           : LOW-COVERAGE-NO-ADVERSE-SIGNAL
Risk score        : 0/100
Confidence        : 45%
Provider agreement: no-adverse-convergence
Provider coverage : 25.0%
Not configured    : AbuseIPDB, ThreatFox, Spamhaus DQS
Interpretation     : Reputation is evidence-based and time-sensitive. No-significant-adverse-signal d
es not mean that the IP is guaranteed safe.

Evidence fusion
---------------
Status            : OK
Unique evidence   : 38
Duplicates removed: 0
Unique sources    : 33
Coverage          : 90.0%
Evidence quality  : 85.2%
  identity     coverage=100.0% quality=100.0% evidence=3
  routing      coverage=100.0% quality=98.6% evidence=5
  geolocation  coverage=100.0% quality=97.8% evidence=4
  dns-tls      coverage=100.0% quality=95.6% evidence=6
  exposure     coverage=100.0% quality=86.7% evidence=18
  reputation   coverage=100.0% quality=85.0% evidence=2
  trace        coverage=0.0% quality=0.0% evidence=0
```

```
Geo consensus
-------------
Country           : DE Germany | consensus 98%
Region            : Hesse | consensus 76%
City              : Frankfurt am Main | consensus 85%
Coordinates       : 50.109179, 8.657732
Provider spread   : 2.12 km
Estimated radius  : 100.0 km [provider-spread-heuristic]
Disagreements     : 1
Precision         : infrastructure-level only

Reverse DNS intelligence
------------------------
Status            : OK
PTR name(s)       : ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
Forward confirmed : no
Resolver(s)       : 127.0.0.53
  ec2-3-72-171-177.eu-central-1.compute.amazonaws.com -> 172.31.42.227

DNS associations
----------------
Status            : OK
Scope             : current-dns
PTR               : ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
CNAME             : -
Zone(s)           : eu-central-1.compute.amazonaws.com
NS                : ns0.eu-central-1.compute.internal
Associated names  : ec2-3-72-171-177.eu-central-1.compute.amazonaws.com, eu-central-1.compute.amazonaw
s.com, ns0.eu-central-1.compute.internal
MX                : -
Passive DNS       : not configured

TLS certificate intelligence
----------------------------
Status            : OK
SNI               : ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
Certificates      : 1
Associated domains: www.ideo-lab.com

Port 443
  TLS version     : TLSv1.3
  Cipher          : TLS_AES_256_GCM_SHA384
  CN              : www.ideo-lab.com
  SAN DNS count   : 1
  Issuer          : countryName=US, organizationName=Let's Encrypt, commonName=YE2
  Serial          : 066C8AF475B9E7207CF35C760EE274E35FE5
  Valid from      : Aug 29 06:43:58 2026 GMT
  Valid until     : Nov 27 06:43:57 2026 GMT
  Key type        : EC
  Signature       : ecdsa-with-SHA384
  SHA-256         : 5241007B41FA0188D25C94219EF21C98C08937CFB293093DB14E4F76468ED6BB

Passive Internet exposure
-------------------------
Status            : OK
Provider          : Shodan InternetDB
Snapshot          : provider-weekly-snapshot
Observed ports    : 80, 443
Hostnames         : ec2-3-72-171-177.eu-central-1.compute.amazonaws.com, www.ideo-lab.com
CPE(s)            : cpe:/a:f5:nginx
Tags              : cloud
Vulnerability refs: 0 [passive metadata only]
```

```
Network ownership
-----------------
REGISTERED OWNER   : A100 ROW GmbH
ALLOCATED TO       : A100 ROW GmbH
CURRENT OPERATOR   : AMAZON-02 - Amazon.com, Inc.
HOSTING PROVIDER   : unconfirmed
BGP ORIGIN         : AS16509

Ownership verdict
-----------------
INFRASTRUCTURE OWNER : A100 ROW GmbH
NETWORK OPERATOR     : AMAZON-02 - Amazon.com, Inc.
RIR                  : ARIN
CONFIDENCE           : 98%

ASN intelligence
----------------
Routed prefix      : 3.64.0.0/12
Origin ASN(s)      : AS16509
Multi-origin       : no
AS16509            : AMAZON-02 - Amazon.com, Inc.
  Registry country: US
  ASN registry     : IANA 16-bit Autonomous System (AS) Numbers Registry

BGP route intelligence
----------------------
Observed origin    : AS16509
Origin consistent  : yes
Routes observed    : 361
Unique AS paths    : 277
RIS collectors     : 23
Path-adjacent AS   : AS1299, AS2914, AS174, AS24482, AS9002, AS6461, AS8218, AS34549
ASN neighbours     : 452

RPKI / routing security
-----------------------
RPKI verdict       : VALID
AS16509            : VALID (valid)

Geolocation sources
-------------------
ipwhois            : Frankfurt am Main, Hessen, DE
  coordinates       : 50.115524, 8.6841725
ipapi              : Frankfurt am Main, Hesse, DE
  coordinates       : 50.1025, 8.6299
dbip               : Frankfurt am Main, Hesse, DE

Network type
------------
Primary type       : unknown
Confidence         : 0%
```

```
IDEO-Lab Deep IP Intelligence Analyzer
======================================
Version           : 0.11.0
Status            : OK
Profile           : deep
Target            : 3.72.171.177
Address family    : IPv4
Category          : public-global
Category detail   : Public globally routable address
Globally routable : yes
Reverse pointer   : 177.171.72.3.in-addr.arpa
Duration          : 7517.977 ms

Analyzers
---------
ip-input              OK       0.022 ms
rdap                  OK       316.534 ms
  warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers correlate
 those signals later in the run.
asn                   OK       1509.558 ms
bgp                   OK       1909.901 ms
rpki                  OK       119.926 ms
geo                   OK       240.685 ms
network-type          OK       0.103 ms
  warning: No network type reached the minimum evidence threshold.
geo-consensus         OK       0.131 ms
  warning: Geolocation providers disagree on one or more location fields.
reverse-dns           OK       5.279 ms
  warning: PTR name exists, but forward resolution did not return the original target address.
dns-association       OK       6.327 ms
passive-exposure      OK       21.721 ms
service-exposure      OK       0.054 ms
reputation-sources    OK       374.862 ms
abuse-signals         OK       0.06 ms
reputation-consensus OK       0.046 ms
  warning: Reputation consensus has fewer than two evaluable provider responses.
tls                   OK       2.861 ms
active-exposure       OK       3004.448 ms
  warning: TCP connect validation tests reachability only; it does not authenticate or exploit any ser
vice.
evidence-fusion       OK       0.27 ms
coherence-engine      OK       0.058 ms
  warning: Geolocation providers disagree
correlation-engine    OK       0.243 ms
  warning: Correlation engine retained 1 unresolved contradiction(s).
historical-intelligence OK       4.606 ms

RDAP / RIR
----------
RIR               : ARIN
IP range          : 3.64.0.0 - 3.79.255.255
CIDR              : 3.64.0.0/12
NetName           : AMAZON-FRA
Organization      : A100 ROW GmbH
Registration      : 2020-10-22T14:19:10-04:00
Last update       : 2020-10-22T14:19:10-04:00
Status            : active
Abuse contacts    : Amazon Web Services, LLC <trustandsafety@support.aws.com>
Technical contacts: Amazon Webservices EC2 <amzn-noc-contact@amazon.com>; Amazon Web Services, LLC <am
zn-noc-contact@amazon.com>; Amazon <ipmanagement@amazon.com>
```

IP-INTEL-012C

— INVESTOR-GRADE VISUALIZATION

Institutional-grade intelligence. Verified. Contextual. Actionable.

VISUALIZATION SHOWCASE

- OVERVIEW
- GEO
- OWNERSHIP
- ASN/BGP
- TRACE
- DNS
- TLS
- SERVICES
- THREATS
- HISTORY
- EDDENCE
- EVIDENCE

INVESTOR-GRADE INTELLIGENCE
TRANSPARENT | VERIFIED | RELIABLE

GEO DISTRIBUTION



United States	42%
Germany	23%
Singapore	14%
Netherlands	8%
Other	13%

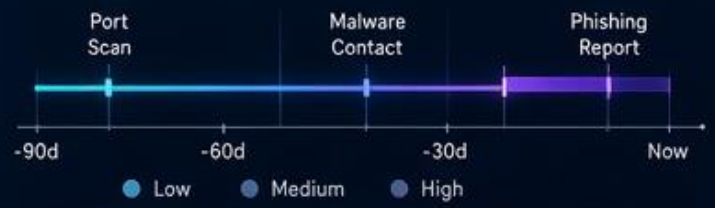
RISK & CONFIDENCE GAUGE



STRONG

Data Quality • Cross-Validated

THREAT TIMELINE



ASN / BGP GRAPH



4 Direct Peers • 12 Announced Prefixes

TRACEROUTE VISUALIZATION



CONFIDENCE BADGE

HIGH CONFIDENCE
87 / 100

- Multi-source validation
- Low volatility
- No conflicts

VISIBLE CONTRADICTIONS

TLS CERT MISMATCH
Certificate CN: *.example.com
Observed Host: 104.21.35.45

CONTRADICTION DETECTED

MINI-MODAL EXPLANATION

WHY THIS MATTERS

This IP belongs to a network with elevated risk indicators and visible inconsistencies.

INVESTOR IMPLICATION

Increased scrutiny recommended. Verify control, ownership, and operational risk before capital allocation.

All data verified from multiple independent sources. Last updated: 2025-05-21 10:24 UTC

IDEO-LAB IP INTELLIGENCE

IP-INTEL-012C • INVESTOR-GRADE INTELLIGENCE

REAL TARGET 3.72.171.177

UPDATED 2 MIN AGO

SCAN

- OVERVIEW
- GEO
- OWNERSHIP
- ASN/BGP
- TRACE
- DNS
- TLS
- SERVICES
- THREATS
- HISTORY
- EVIDENCE

DATA SOURCES
17 OSINT + PROPRIETARY

GEO DISTRIBUTION

Germany / Frankfurt

98% CONFIDENCE



Frankfurt (FRA) • eu-central-1

DATA SOURCES 12

RISK & CONFIDENCE GAUGE



LOW OBSERVED RISK PROFILE

Based on 30-day observation window

THREAT TIMELINE

STABLE • NO MALWARE SPIKES



ASN/BGP GRAPH

ORIGIN AS16509 • Amazon.com



IPv4 PREFIXES 1,024

PEERS 128

UPTIME 99.99%

HIJACK MONITOR CLEAN

TRACEROUTE

TARGET 3.72.171.177 • Frankfurt, Germany

REACHED DESTINATION

HOP	IP ADDRESS	RTT	NODE
1	192.168.1.1	0.6 ms	Your Gateway
2	10.0.0.1	1.2 ms	ISP Edge
3	212.34.56.78	8.7 ms	Upstream Transit
4	193.34.27.1	12.4 ms	Peering Node
5	52.93.120.10	14.1 ms	AWS Edge
6	3.72.171.177	14.8 ms	Destination

PATH TERMINATES AT AWS
eu-central-1

Frankfurt, Germany
eu-central-1

CONFIDENCE BADGE



HIGH CONFIDENCE

Multi-source corroborated

- ✓ GEO • 12 sources
- ✓ ASN/BGP • 8 sources
- ✓ TLS • Valid
- ✓ DNS • Consistent

LAST VALIDATED 2 MIN AGO

VISIBLE CONTRADICTIONS

DETECTED ANOMALIES

GEO_PROVIDER_DISAGREEMENT — MEDIUM
2 providers report non-EU locations

PTR_FORWARD_MISMATCH — MEDIUM
Reverse DNS does not match forward.

Impact: Minor • Review recommended

EXPLANATION • INVESTOR IMPLICATION

This IP belongs to AWS Frankfurt (eu-central-1) infrastructure. ASN AS16509, RPKI valid, no hijack alerts, clean threat history, and low observed risk.

Low observed risk is not a safety guarantee.
Infrastructure can change.
Continuous monitoring required.

© IDEO-LAB • IP-INTEL-012C • 2024

IP INTELLIGENCE COCKPIT

STRUCTURE CIBLE

ANALYSED TARGET
3.72.171.177 IPv4
PROFILE
Deep · AWS · Frankfurt

DURATION
7518 ms
CONFIDENCE
89.5/100 HIGH

LIVE UPDATED

RISK SCORE
0 /100
LOW-OBSERVED-RISK

CONFIDENCE
89.5 /100

COHERENCE
96 /100

EVIDENCE QUALITY
85.2 /100

GEO DISTRIBUTION

Frankfurt am Main
Hesse
DE
98%



COORDS 50.109179, 8.657732
SPREAD 2.12 km

RISK & CONFIDENCE



CONFIDENCE
89.5/100

OBSERVATION / THREAT TIMELINE



HISTORICAL UNCHANGED
2 SNAPSHOTS · STABLE

ASN / BGP

AS16509
Amazon ACTIVE



PREFIX	3.64.0.0/12
RPKI	VALID
ORIGIN	CONSISTENT
ANNOUNCED	NOW
PEERS VISIBLE	152

OWNERSHIP

A100 ROW GmbH OPERATOR

OPERATOR	AMAZON-02
RIR	ARIN
REGISTRATION	2013-08-21

RELATIONSHIP
CUSTOMER

TLS / SERVICES

80 / 443 OPEN

SERVICE	f5 / nginx
CN	www.ideo-lab.com
TLS	TLS 1.3
CERT	Let's Encrypt

VISIBLE CONTRADICTIONS

DETECTED

- GEO_PROVIDER_DISAGREEMENT
- PTR_FORWARD_MISMATCH
- DNS_TLS_NAME_DIVERGENCE

REPUTATION COVERAGE 25%

MINI EXPLANATION SYNTHESIS

- BGP consistent
- RPKI valid
- Geo located in DE
- Risk score 0/100

One contradiction remains visible (1)

SYNTHESIS Strong infrastructure coherence, low risk posture, stable history — one resolver-level naming/geolocation contradiction remains visible.

DATA FRESHNESS 28 s ago LIVE

ASN / BGP GRAPH

IP INTELLIGENCE DASHBOARD



ROUTES
361

AS PATHS
277

COLLECTORS
23

NEIGHBOURS
452

ORIGIN CONSISTENT YES

RPKI VALID

DATA SOURCE: RIPE RIS | UPDATED: LIVE

INVESTOR-GRADE INTELLIGENCE

Ce que le premier scan donnera — HISTORICAL INTELLIGENCE

CURRENT MODE	SNAPSHOTS	CURRENT SNAPSHOT	RISK TREND
HISTORICAL INTELLIGENCE	Comparing first scan scenarios	First Scan (Baseline)	Projected from first scan

1 BASELINE

First scan reference state



OK

MODE	Historical Intelligence
SNAPSHOT	First Scan (Baseline)
PREVIOUS RISK	—
DELTA RISK	—
CONFIDENCE	High
RISK TREND	Stable

BASELINE

2 SECOND SCAN

Projected second scan outcome



UNCHANGED

MODE	Historical Intelligence
SNAPSHOT	Second Scan (Projected)
PREVIOUS RISK	Baseline
DELTA RISK	0%
CONFIDENCE	High
RISK TREND	Stable

STABLE

3 IF BGP CHANGES

Projected outcome with BGP routing changes



CHANGED

MODE	Historical Intelligence
MATERIAL CHANGES	Yes
COVERAGE CHANGES	Expanded
HIGHEST SEVERITY	High
CHANGED SECTIONS	Routing, Peers, Paths
RISK / CONFIDENCE DELTA	+18% / -12%
RISK TREND	Increasing

RECOMPUTED / INCREASING

BATCH12
DASHBOARD FINAL DECISIONNEL
GENRE COCKPIT AVION

IDEO-LAB DEEP IP ANALYZER | TARGET 3.72.171.177 | IPv4 PUBLIC-GLOBAL | PROFILE DEEP | STATUS OK | 15.8 s | LIVE

RISK 0/100



LOW-OBSERVED-RISK

CONFIDENCE	97.4%	HIGH
COHERENCE	96%	HIGH
EVIDENCE QUALITY	94.8%	HIGH
COVERAGE	100%	

NAVIGATION DISPLAY

GEO



OWNERSHIP

ORG	A100 ROW GmbH
OPERATOR	Amazon
RIR	ARIN
CONFIDENCE	98%

EXPOSURE

PORTS	80/443 OPEN	80 f5	443 nginx
TLS	TLS1.3	CN	www.ideo-lab.com

TRACE

244.5.0.107 → 3.72.171.177 (DEST)

RTT	0.222 ms	REACHED	YES
METHOD AGREEMENT	0%		

CAUTION / WARNING

GEO_PROVIDER_DISAGREEMENT | PTR_FORWARD_MISMATCH | DNS_TLS_NAME_DIVERGENCE | TRACE_METHOD_DIVERGENCE | REPUTATION_LOW_COVERAGE 25%

HISTORICAL RISK DELTA 0.0 | MODE CHANGED LOW | SEVERITY LOW | TRACE PATH FINGERPRINT CHANGED | SNAPSHOTS 4

SYNTHESIS BGP and RPKI coherent, geo DE, no adverse technical risk; low risk is not a safety guarantee.


IDEO-LAB IP ANALYZER
ENG
3.72.171.177
DEEP
STATUS OK
15.8s
1
RISK
0%
LOW-OBSERVED
2
CONFIDENCE
97%
HIGH
3
COHERENCE
96%
HIGH
4
EVIDENCE Q
95%
HIGH
5
GEO CONSENSUS
98%
DE
FRANKFURT
6
REPUTATION COV
25%
LOW COVERAGE
OWNERSHIP CONF
98%
RPKI
VALID
ORIGIN CONSISTENT
YES
TRACE METHOD AGREE
0%
TRACE RTT
0.222 ms
PORTS
80/443 OPEN
GEO_PROVIDER_DISAGREEMENT
PTR_FORWARD_MISMATCH
DNS_TLS_NAME_DIVERGENCE
TRACE_METHOD_DIVERGENCE
HIST MODE CHANGED
TRACE PATH FINGERPRINT
SEV LOW
SNAPSHOTS 4
RISK DELTA 0.0
AS16509
AMAZON-02
PREFIX 3.64.0.0/12
A100 ROW GmbH
FRANKFURT.

IDEO-LAB
IP INTELLIGENCE SUITE

- OVERVIEW
- GEO
- OWNERSHIP
- ASN/BGP
- TRACE
- DNS
- TLS
- SERVICES
- THREATS
- HISTORY
- EVIDENCE

IP-INTEL-012C
v2.7.1 • INVESTOR GRADE

IDEO-LAB IP INTELLIGENCE

REAL TARGET 3.72.171.177 UPDATED LIVE 00:00:03 ago

SCAN

GEO DISTRIBUTION



Germany
Frankfurt
98%
eu-central-1

RISK & CONFIDENCE

Confidence
97.4
HIGH

Risk
0/100
LOW-OBSERVED-RISK

THREAT TIMELINE

STABLE
No malware spikes detected.



HISTORICAL RISK DELTA 0.0

ASN/BGP GRAPH



PREFIX 3.64.0.0/12 | NEIGHBOURS 458 | RPKI VALID
ORIGIN CONSISTENT

TRACEROUTE

1 — 2

1 244.5.0.107
Frankfurt (DE)

3.72.171.177
Destination

RTT
0.222 ms

REACHED
YES

METHOD AGREEMENT 0% | PATH TERMINATES
AWS eu-central-1 Frankfurt

CONFIDENCE BADGE

97.4
/100

HIGH CONFIDENCE
Strong infrastructure consistency observed.

DATA FRESHNESS: LIVE

VISIBLE CONTRADICTIONS

GEO_PROVIDER_DISAGREEMENT
Low impact

PTR_FWD_MISMATCH
Low impact

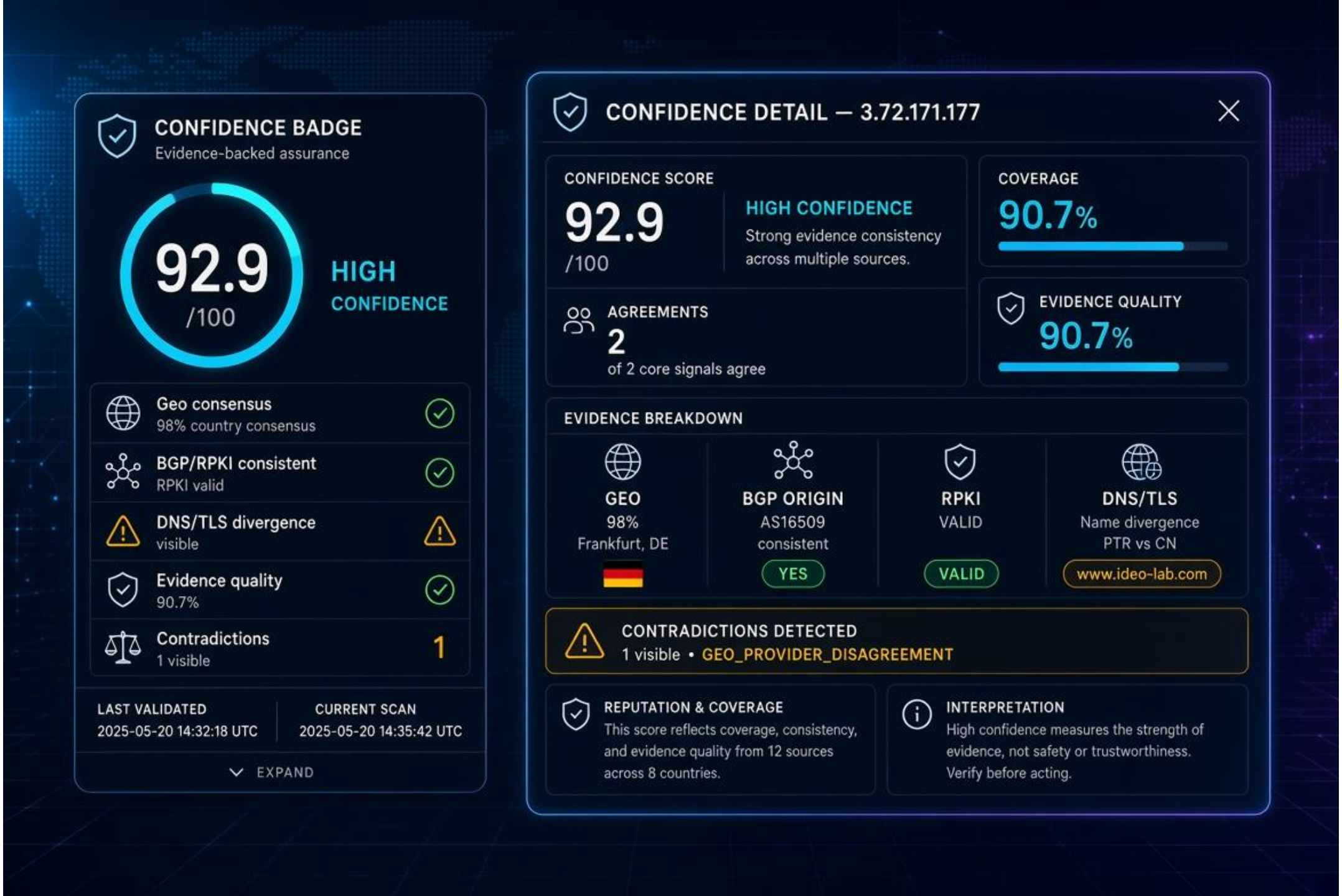
DNS_TLS_NAME_DIVERGENCE
Low impact

TRACE_METHOD_DIVERGENCE
Low impact

REPUTATION COVERAGE
25%

AWS Frankfurt infrastructure

✓ RPKI valid
Historical mode: CHANGED on TRACE PATH FINGERPRINT
Severity: LOW
Snapshots: 4
Low observed risk is not a safety guarantee.


CONFIDENCE BADGE
Evidence-backed assurance
92.9
/100
HIGH
CONFIDENCE
Geo consensus
98% country consensus
BGP/RPKI consistent
RPKI valid
DNS/TLS divergence
visible
Evidence quality
90.7%
Contradictions
1 visible
1
LAST VALIDATED
2025-05-20 14:32:18 UTC
CURRENT SCAN
2025-05-20 14:35:42 UTC
EXPAND
CONFIDENCE DETAIL — 3.72.171.177
CONFIDENCE SCORE
92.9
/100
HIGH CONFIDENCE
Strong evidence consistency across multiple sources.
COVERAGE
90.7%
AGREEMENTS
2
of 2 core signals agree
EVIDENCE QUALITY
90.7%
EVIDENCE BREAKDOWN
GEO
98%
Frankfurt, DE
BGP ORIGIN
AS16509
consistent
YES
RPKI
VALID
VALID
DNS/TLS
Name divergence
PTR vs CN
www.ideo-lab.com
CONTRADICTIONS DETECTED
1 visible • GEO_PROVIDER_DISAGREEMENT
REPUTATION & COVERAGE
This score reflects coverage, consistency, and evidence quality from 12 sources across 8 countries.
INTERPRETATION
High confidence measures the strength of evidence, not safety or trustworthiness. Verify before acting.


COHERENCE & CONTRADICTIONS
OK System coherence is within normal bounds.
96%
COHERENCE
AGREEMENTS
5
CONTRADICTIONS
1
OBSERVATIONS
4
GEO_PROVIDER_DISAGREEMENT
WARNING
EXPAND
COHERENCE DETAIL
CONTRADICTION
[MEDIUM]
GEO_PROVIDER_DISAGREEMENT
geolocation consensus reports 1 disagreement.
OBSERVATIONS (4)
PTR_FORWARD_MISMATCH
Reverse DNS does not forward-confirm.
DNS_TLS_NAME_DIVERGENCE
DNS and TLS names differ.
REPUTATION_LOW_COVERAGE
Reputation coverage is limited.
NETWORK_TYPE_UNRESOLVED
Network type remains unresolved.
TRACE COVERAGE
100%
COVERAGE
93.7%
QUALITY
6
EVIDENCE

WHY THIS MATTERS

LOW-OBSERVED-RISK

Context before conclusion

KPI SUMMARY (AT A GLANCE)

RISK
0/100
LOW

CONFIDENCE
89.5%
HIGH

COHERENCE
96.0%
HIGH

EVIDENCE QUALITY
85.2%
HIGH

INTERPRETATION (SHORT)

Risk measures adverse technical signals.
Confidence measures how strongly the available evidence supports the synthesis.

- 0 material risk drivers
- Confidence is evidence strength not proof of safety

EXPAND

WHY THIS MATTERS — INTERPRETATION

KPI SUMMARY (DETAILED)



INTERPRETATION

Overall risk is low based on available signals. The synthesis is supported by strong, coherent evidence of high quality, though some external validation paths remain incomplete. This is an evidence-based low-risk view, not a guarantee of future outcomes.

CURRENT LIMITATIONS

- No evaluable trace core evidence is available
- Reputation coverage is limited to 25.0%
- PTR forward-confirmation is incomplete
- DNS-derived names and certificate names differ

0 material risk driver(s)

Confidence is evidence strength, not proof of safety.

Geolocation intelligence

Consensus first · source-level observations visible

3 sources · 1 disagreement

Location consensus

50.11°N 8.68°E · City-level lock



COUNTRY

Germany

98% Country confidence

REGION

Hesse

CITY

Frankfurt am Main

SOURCES

3 providers

1 disagreement

Provider observations

Provider	Country	Region	City	Latitude	Longitude	Status
ipwhois	DE	Hesse	Frankfurt am Main	50.115524	8.6841725	consensus
ipapi	DE	Hesse	Frankfurt am Main	50.1025	8.6299	consensus
dbip	DE	Hesse	Frankfurt am Main	—	—	partial

Dashboard user: contact@ideo-lab.com · IP Analyzer history is isolated inside this user's Security Analyzer workspace.

Ownership & network identity

Registry ownership remains separate from current network operation.

A100 ROW GmbH

Registered owner | Allocated to | Infrastructure owner

Same legal entity across registry fields

AMAZON-FRA

ARIN Registry

Registry record

RIR	ARIN (ARIN)
Registered owner	A100 ROW GmbH
Allocated to	A100 ROW GmbH
Infrastructure owner	A100 ROW GmbH

Network operation

Current operator	Not observed
Network type	Unknown
Prefix	Not published

Whois registry identity does not confirm the live operator.

Likely AWS Frankfurt naming (AMAZON-FRA) while the ARIN registrant is A100 ROW GmbH — treat registry and routing operation as separate evidence.

ASN / BGP / RPKI

Routing origin, consistency and trace-derived ASN path.

AS16509

Amazon.com, Inc.

AMAZON-02

Registry country US

IANA

IANA 16-bit AS Numbers Registry

RPKI VALID

Origin consistent

Multi-origin: no

Routed prefix

3.64.0.0/12

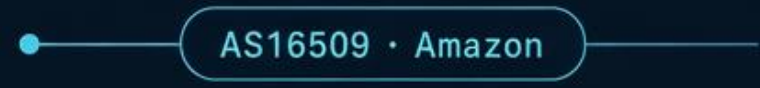
Routes observed	Unique AS paths	RIS collectors	ASN neighbours
360	276	23	455

Origin alignment

Routed prefix	3.64.0.0/12	
Registry origin ASN	AS16509	
Observed BGP origin	AS16509	
Origin consistent	Yes	
Trace ASN path	AS16509	
Current operator	—	treated as aligned to Amazon

Registry origin and live BGP origin match.

Observed ASN path



Trace-derived path (1 hop / origin only)

Path-adjacent AS

AS1299 | AS2914 | AS174 | AS24482 | AS9002 | AS6461 | AS8218 | AS34549

455 neighbours total · showing adjacent set from RIS

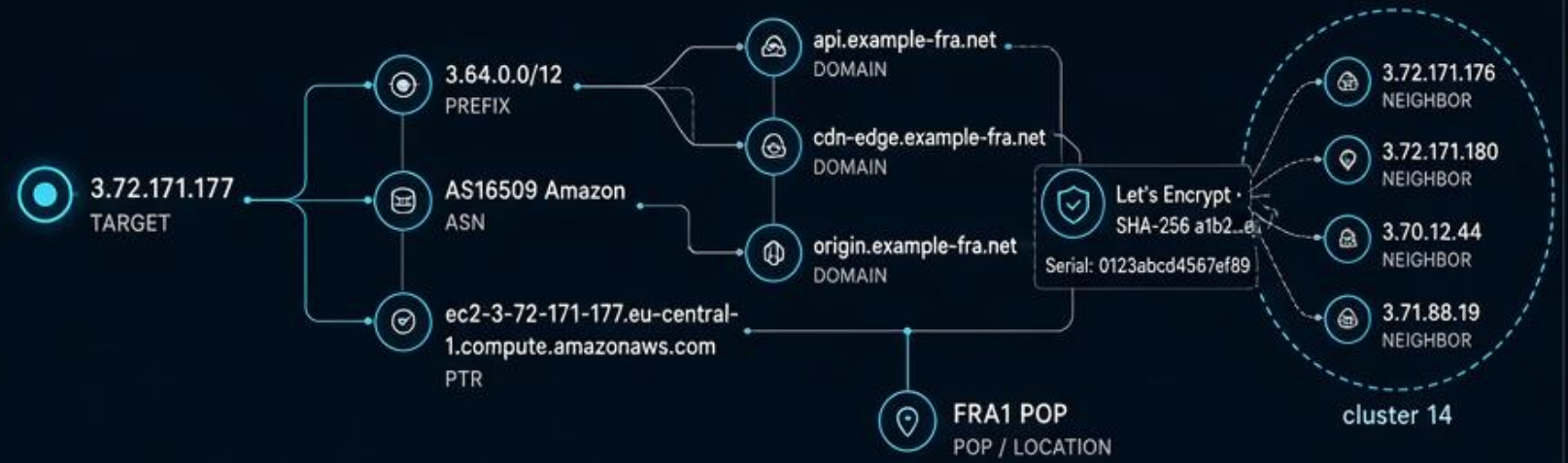
Shared infrastructure graph

IP-INTEL-016

IP → prefix → ASN → PTR → DNS domains → TLS certs → other IPs. Investigation mode, not a score.

14 IPs | 3 domains | 1 Let's Encrypt cert | 1 ASN (AS16509) | 1 Frankfurt POP

Seed IP highlighted: 3.72.171.177 · prefix 3.64.0.0/12 AMAZON-FRA



Pivots used

- ✓ Same cert serial SHA-256
- ✓ Same SANs
- ✓ Same NS / SOA
- ✓ Same HTTP title + favicon hash (passive)
- ✓ Same traceroute path signature
- ✓ Same BGP upstreams

Cluster members

IP	Role	Pivot
3.72.171.177	seed	—
3.72.171.176	neighbor	cert + PTR
3.72.171.180	neighbor	cert + SAN
3.70.12.44	same cert	SHA-256
3.71.88.19	same NS/SOA	dns

ⓘ Note: Batch 13C IP A vs IP B is a 2-node special case of this cluster.

ⓘ Output: 14 IPs, 3 domains, 1 Let's Encrypt cert, 1 ASN, 1 Frankfurt POP — shared infrastructure, not an isolated host.

Traceroute visualization

Explain

Consensus hops use real active trace evidence only.

Destination reached: YES | Hop estimate: 2 | Method agreement: 0% | Divergent hops: 1 | Successful vantages: 0 | Multi-vantage verdict: Not observed



sig: 244.5.0.111 → 3.72.171.177/AS16509

Hop table

#	Address	ASN	Geo	RTT	Notes
1	244.5.0.111	—	—	1.758 ms	reserved space, not a public transit hop
2	3.72.171.177	AS16509	DE	0.184 ms	destination, AWS eu-central-1

Evidence quality

- Active trace: destination reached
- Method agreement 0% — ICMP/UDP/TCP did not corroborate the same hop set
- Divergent hops: 1
- Multi-vantage: 0 successful vantages — single-probe path only, do not treat as internet-wide path
- Note: first hop in 244.0.0.0/8 (Class E reserved). Treat as vantage/internal or artifact, not a public router.

Short 2-hop path to AS16509 in DE. Useful as a path signature for clustering, but weak as multi-vantage routing evidence.

DNS & TLS intelligence

PTR, associated names and certificate observations — infrastructure names vs tenant names.

IP

3.72.171.177

VERDICT

CLOUD VIRTUAL HOSTING

PTR / SNI = AWS EC2 hostname
Certificate CN = www.ideo-lab.com
PTR forward-confirmed: NO
Not a bug — cloud instance + virtual host

INFRA NAMES (AWS)

PTR:	ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
Forward-confirmed:	No (amber chip) — A/AAAA does not point back to 3.72.171.177.
TLS SNI:	ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
Zone:	eu-central-1.compute.amazonaws.com
Associated:	eu-central-1.compute.amazonaws.com · ns0.eu-central-1.compute.internal

TENANT NAMES

TLS domain / cert CN:	www.ideo-lab.com
Role:	virtual host on this instance
Link:	see IP-INTEL-017 for historical PDNS/CT

CERTIFICATE

Port	CN	Issuer	Valid until	SAN (implied)	Status
443 · TLSv1.3	www.ideo-lab.com	Let's Encrypt (YE2) · US	27 Nov 2026 06:43 GMT	www.ideo-lab.com	valid, not expired

PTR / SNI ec2-...amazonaws.com — divergence expected on cloud virtual hosting — Certificate CN www.ideo-lab.com

INSIGHT Do not treat PTR as the site name. Verify the virtual host (www.ideo-lab.com). PTR not forward-confirmed is common on EC2 and must stay visible.

Internet exposure & services

Passive observations stay distinct from bounded active validation.

3.72.171.177 · www.ideo-lab.com

tag cloud CPE cpe:/a:f5:nginx product f5/nginx

- Service exposure: OK
- Observed services: 2
- New active ports: none
- Active validation: OK
- Review priority HIGH=0 REVIEW=0 NORMAL=2
- Guardrail chip: tcp-connect-only · no exploit payloads

PASSIVE

Ports	80, 443 confirmed
Hostnames:	ec2-3-72-171-177.eu-central-1.compute.amazonaws.com www.ideo-lab.com
Passive not now:	none
Status	OK

ACTIVE VALIDATION

Scope:	TCP connect-only
Open TCP:	80, 443
Closed TCP:	none observed in this probe set
Indeterminate (timeout / filtered):	21, 22, 25, 53, 110, 143, 445, 587, 993, 995
Newly observed:	none
Passive confirmed matches open:	80, 443

PORT	SERVICE	CATEGORY	PRIORITY	VALIDATION STATE
80	http	web	priority normal	passive+active agree
443	https	web	priority normal	passive+active agree TLS 1.3

Open (confirmed) 80 443 | Indeterminate (not closed — not proven open) 21 22 25 53 110 143 445 587 993 995

Insight No HIGH/REVIEW services. Active scan did not invent new ports. Indeterminate ≠ closed. Product is f5/nginx on cloud — aligns with origin web / reverse-proxy role.

Threat intelligence

Provider signals are time-sensitive and are not attribution proof. Absence of hits is not safety.

● 3.72.171.177 • www.ideo-lab.com • AS16509

VERDICT

LOW-COVERAGE-NO-ADVERSE-SIGNAL

Agreement: no-adverse-convergence

Adverse providers: 0

Risk score	Confidence	Providers evaluated
0/100	45%	1 of 4
— covered set only	— low because coverage is thin	— out of available feeds

Coverage 25%

absence ≠ safe

PROVIDER	STATUS	OBSERVED	SIGNAL	MEANING
GreyNoise Community	not-found	no	—	Evaluated. No classification / not seen. Unseen ≠ benign.
AbuseIPDB	not-configured	no	—	Coverage gap. Silence is not a clear.
ThreatFox	not-configured	no	—	Coverage gap.
Spamhaus ZEN	not-configured	no	—	Coverage gap

No adverse provider signal in the evaluable set (GreyNoise only).

This is not proof that the IP is safe.

Recommended print: No adverse IOC on 1/4 providers; 3 feeds uncovered; do not treat 0/100 as clean.

Coverage callout: Enable AbuseIPDB, ThreatFox, Spamhaus to raise confidence above 45%.

LOW-COVERAGE-NO-ADVERSE-SIGNAL is the honest class. 0 adverse + 1 provider evaluated = low confidence, not a green bill of health.

Historical intelligence

Material state changes remain separate from coverage changes.

- Target: 3.72.171.177
- 12 snapshots
- first seen 16 Sep 2026 20:05 UTC
- previous 17 Sep 13:53 UTC
- latest 17 Sep 20:34 UTC

MODE: changed

Risk delta	Confidence delta	Material changes	Coverage changes
0.0	+3.4 (89.5 → 92.9)	3	1

⚠ Latest snapshot #21 is PROFILE=trace. Trace does not populate Origin ASN / operator. Apparent HIGH "Origin ASN [16509] → [] MEDIUM/ AMAZON-02 → empty" are COVERAGE changes, not a routing event. Class: COVERAGE_GAP_ON_TRACE_PROFILE — do not alert as ASN withdrawal.

TIMELINE



#20 last full deep with AS16509

quick deep trace

CHANGES

COVERAGE (1)

- Origin ASN set removed [16509] → [] — cause: trace profile
- Operator AMAZON-02 → "" — same cause."

MATERIAL / LOW

- Correlation confidence increase 89.5 → 92.9 severity low
- Risk unchanged 0

SNAPSHOT HISTORY

ID	DATE (UTC)	PROFILE	RISK	CONFIDENCE	PORTS		ORIGIN ASN
#21	17 Sep 20:34	trace	0	92.9	80,443	—	coverage hole
#20	17 Sep 13:53	deep	0	89.5	80,443	—	16509
#19	17 Sep 13:31	quick	0	89.8	80,443	—	16509
#2	16 Sep 12:55	quick	0	85.4	80,443	—	—
#1	16 Sep 20:06	quick	0	89.8	80,443	—	16509

12 of 21 ids kept — gaps are dropped runs

ⓘ *Insight: Same IP, risk flat. Do not page on ASN disappearing after a trace-only run. Compare deep-to-deep for material topology.*

Evidence summary

Evidence quality, contradictions and risk drivers without the raw record wall.

Explain

Target: 3.72.171.177 ● fusion status OK

Unique evidence	Unique sources	Coverage	Evidence quality
43	36	93.3%	90.7%
deduplicated · 0 duplicates removed	independent inputs	profile coverage	weighted

FAMILY QUALITY GRID (from fusion engine, compact bars)

family	coverage	quality	evidence count
identity	cov 100%	q 100%	n=3
routing	cov 100%	q 98.6%	n=5
geolocation	cov 100%	q 97.8%	n=4
dns-tls	cov 100%	q 95.6%	n=6
trace	cov 100%	q 95.7%	n=6
exposure	cov 100%	q 86.7%	n=18
reputation	cov 100%	q 85.0%	n=2

Exposure and reputation slightly lower quality — still covered.

VISIBLE CONTRADICTIONS — 1 retained

Geolocation providers disagree

Consensus	1 disagreement
Sources	geo, geo-consensus
Interpretation	infrastructure-level / AWS region vs city providers — do not treat as street-level conflict
Link	Geo tab · class already known from cloud-calibrated geo

RISK DRIVERS — 0 material

No material adverse technical risk driver currently observed.

Aligns with Threats LOW-COVERAGE-NO-ADVERSE-SIGNAL.

Insight: 43 evidence items, 1 geo disagreement, 0 risk drivers. Quality is weakest on reputation (85%) and exposure (86.7%) — coverage is not the problem.

BATCH 13

IP-INTEL-013A — JSON Evidence Report

Format structuré exploitable par d'autres applications.

IP-INTEL-013B — Human Readable Report

Rapport détaillé avec :

```
Executive Summary
Ownership
Routing
Location
DNS
TLS
Exposure
Threat Intelligence
Trace
History
Evidence
```

IP-INTEL-013C — Comparison Mode

Très intéressant :

```
IP A versus IP B
```

On pourra rechercher des relations :

```
same ASN
same provider
same prefix
same certificate
same domains
same route
same infrastructure
```

BATCH 14

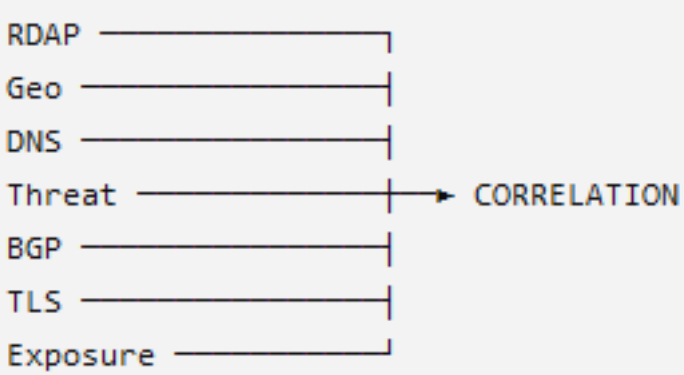
IP-INTEL-014A — Cache / Rate Limit / Resilience

Cache local, retry, expiration, API quota management et gestion des fournisseurs hors ligne.

IP-INTEL-014B — Concurrent Execution

Tous les moteurs indépendants devront pouvoir tourner en parallèle.

Par exemple :



On pourra raccorder cette partie au moteur concurrent du Security Analyzer **après avoir vérifié son état réel d'implémentation**, conformément à notre règle de ne jamais présumer qu'un batch précédent est installé.

IP-INTEL-014C — Production Qualification

Tests :

```
IPv4
IPv6
private IP
public IP
cloud IP
CDN IP
VPN
Tor
mobile
residential
hosting
unreachable IP
invalid IP
API failure
DNS timeout
BGP disagreement
```

avec tests standalone et dashboard.

MOCKUP
SECURITY ANALYZER

IP ANALYZER

Workspace • Security Analyzer



contact@ideo-lab.com | Logout

73%

Workspace readiness

11 views ready · 4 locked

Configure uptime to unlock Availability, Incidents, Status and SLA.

IN PROGRESS

Configure uptime

Start

- Dashboard cockpit — Open
- Launch new scan — RECOMMENDED — Open
- Scan jobs · operational queue — Open

Security scans

Runs 8 runs Ready	Summary Run #48 Ready	Knowledge Catalog ready Action
Findings 98 findings Ready	Attack 69 signals Ready	Timeline 8 comparable runs Ready
Portfolio 6 websites Ready	Compliance 33 tools · 39 metrics Ready	Report Run #48 Ready
Remediate 14 priorities Ready	Risks 98 findings Ready	Compare 8 comparable runs Ready

Uptime modules locked

- Availability
- Incidents
- Status
- SLA

Collect production uptime to unlock these four views.

Configure uptime

Intelligence

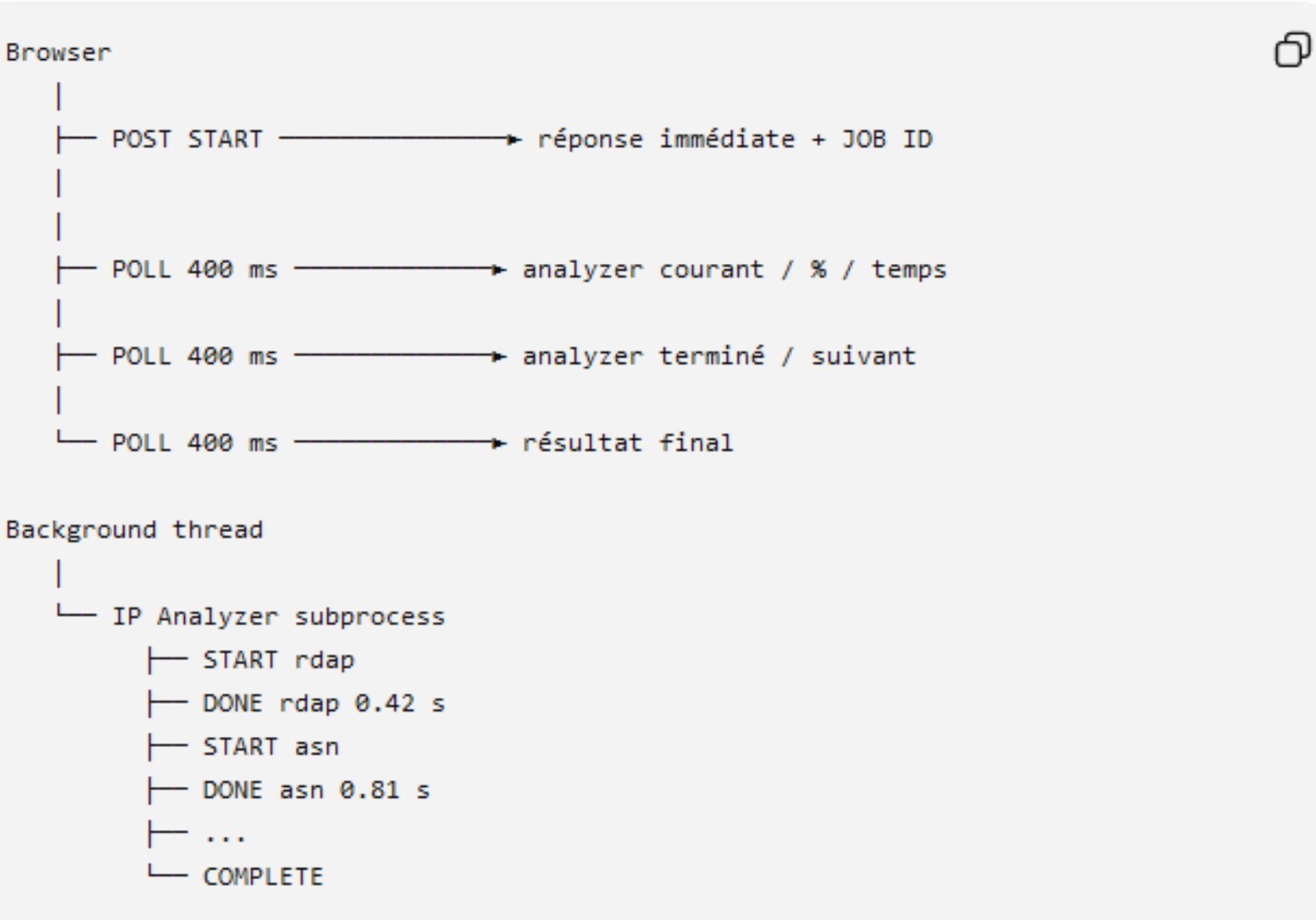
Intel
1 run
Action

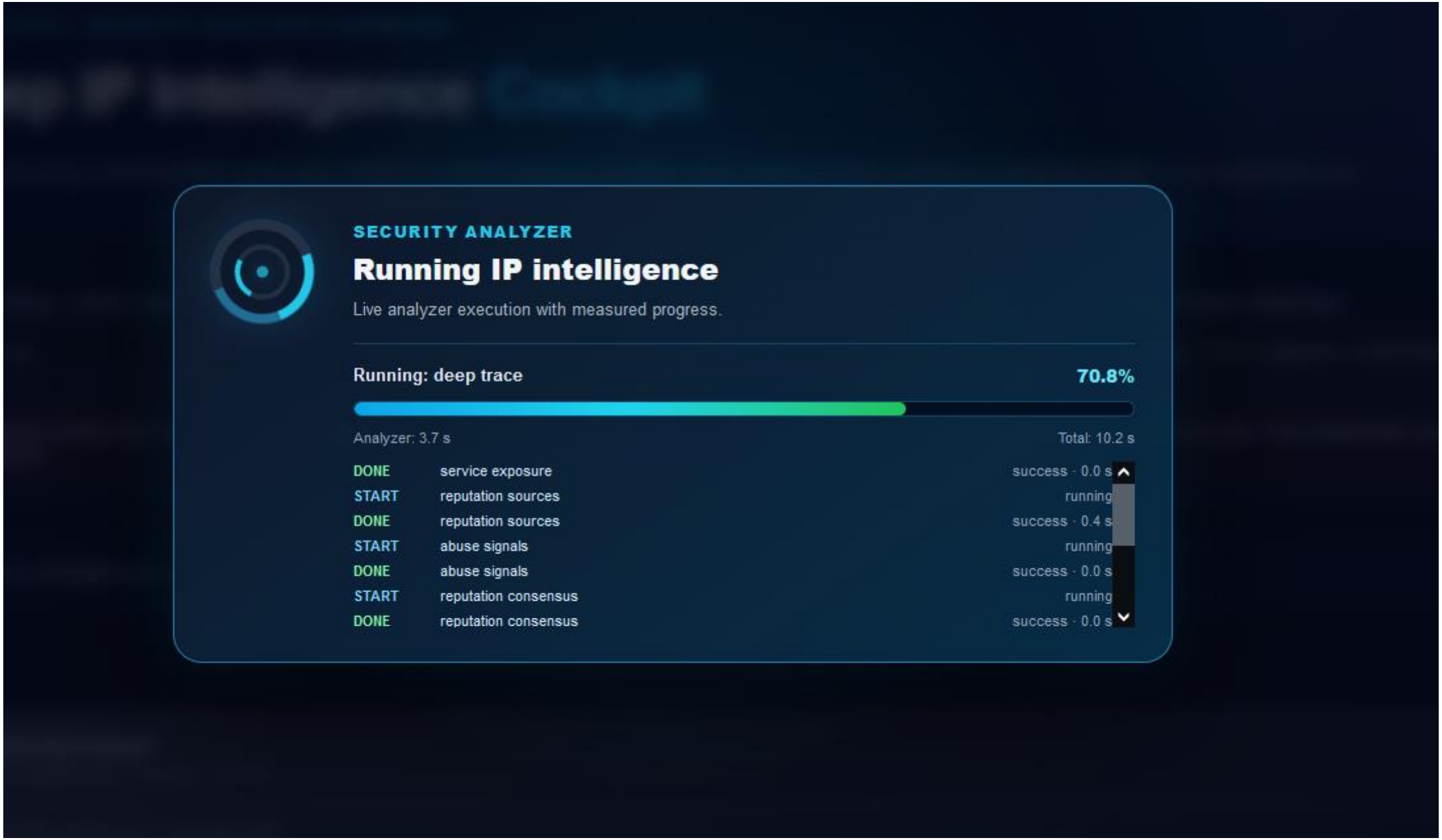
Need help?

Open guided workflow →

IP Analyzer history is isolated inside this user's Security Analyzer workspace.

IP ANALYZER ASYNCHRONE


Browser
POST START
réponse immédiate + JOB ID
POLL 400 ms
analyzer courant / % / temps
POLL 400 ms
analyzer terminé / suivant
POLL 400 ms
résultat final
Background thread
IP Analyzer subprocess
START rdap
DONE rdap 0.42 s
START asn
DONE asn 0.81 s
...
COMPLETE


SECURITY ANALYZER
Running IP intelligence
Live analyzer execution with measured progress.
Running: deep trace
70.8%
Analyzer: 3.7 s
Total: 10.2 s
DONE service exposure success · 0.0 s
START reputation sources running
DONE reputation sources success · 0.4 s
START abuse signals running
DONE abuse signals success · 0.0 s
START reputation consensus running
DONE reputation consensus success · 0.0 s

IP ANALYZER
GPS / REVIEW

AGENDA DES PATCH (18 au total)

- BATCH 1 — IP-GPS-001A / 001B / 001C — Global Assessment Foundation
- BATCH 2 — IP-GPS-002A / 002B / 002C — Grande page IP Global Assessment
- BATCH 3 — IP-GPS-003A / 003B / 003C — Recommendations & Action Engine
- BATCH 4 — IP-GPS-004A / 004B / 004C — Historical Intelligence
- BATCH 5 — IP-GPS-005A / 005B / 005C — Navigation & History Integration
- BATCH 6 — IP-GPS-006A / 006B / 006C — Explanation & Investor UX

BATCH 1 — IP-GPS-001A / 001B / 001C — Global Assessment Foundation

C'est le socle. Pas encore de grosse page spectaculaire, mais il prépare toutes les données nécessaires.

IP-GPS-001A — Assessment Data Aggregator

Créer un moteur qui prend le résultat complet d'un scan IP et le transforme en un objet de synthèse unique :

```
target
profile
scan_id
scan_date
duration
overall_risk
confidence
evidence_quality
good_signals[]
attention_signals[]
critical_signals[]
```

Il ne crée aucune conclusion arbitraire : il consolide ce que disent déjà BGP, RPKI, Reputation, Exposure, TLS, DNS, Geo, Trace, Correlation, etc.

IP-GPS-001B — Important Signal Selector

Créer le moteur qui décide quels éléments méritent réellement d'apparaître dans le GPS.

Exemple : sur 150 éléments techniques, on peut retenir seulement :

```
✓ BGP origin consistent
✓ RPKI valid
! Unexpected exposed service
! Routing path changed
! Reputation source reported adverse evidence
```

Avec pour chaque signal :

```
severity
title
summary
why_it_matters
source_analyzer
source_section
```

IP-GPS-001C — Global Assessment Contract

Créer le contrat de données stable utilisé par toute l'interface :

Python

Exécuter

```
{
    "assessment": {...},
    "signals": {...},
    "recommendations": [...],
    "history_delta": {...},
}
```

Ainsi la future UI ne devra jamais recalculer les conclusions en JavaScript.

BATCH 1 · IP-GPS-001A / 001B / 001C

IP ANALYZER

Global Assessment Foundation — le socle de l'analyse IP

Aucune conclusion arbitraire. On consolide ce que disent déjà les analyseurs.



001A · Data Aggregator

Scan complet → objet de synthèse unique

- target · profile · scan_id · overall_risk
- confidence · evidence_quality
- good_signals[] · attention_signals[]
- critical_signals[]

001B · Signal Selector

150 signaux techniques → seuls ceux qui comptent

- BGP origin consistent
- RPKI valid
- Unexpected exposed service
- Routing path changed

001C · Assessment Contract

Contrat stable pour toute l'UI

```
{
  "assessment"
  "signals"
  "recommendations"
  "history_delta"
}
```

La UI ne recalcule jamais les conclusions.

RISK & CONFIDENCE



confidence **86%**

evidence_quality **HIGH**

SIGNAL GROUPS

GOOD	2
ATTENTION	3
CRITICAL	1

Consolide BGP · RPKI · Reputation · Exposure · TLS · DNS · Geo · Trace · Correlation — un objet, des signaux, un contrat.

BATCH 2 — IP-GPS-002A / 002B / 002C — Grande page IP Global Assessment

Là on obtient le premier résultat spectaculaire.

IP-GPS-002A — Global Assessment Page

Création de la vraie page :

IP GLOBAL ASSESSMENT — 3.72.171.177

avec gros blocs :

```
RISK
CONFIDENCE
STATUS
EVIDENCE QUALITY
```

et identité rapide :

```
ASN / Operator
Country / region
Profile
Last scan
Execution time
```

IP-GPS-002B — Good / Attention / Important

Ajout des trois grandes zones visuelles :

```
GOOD / REASSURING
NEEDS ATTENTION
IMPORTANT
```

Uniquement les signaux réellement présents.

Chaque ligne sera cliquable pour ouvrir son explication.

IP-GPS-002C — What You Should Know

Une section extrêmement lisible :

WHAT YOU SHOULD KNOW

avec les 5–10 faits essentiels classés par importance.

C'est véritablement le résumé exécutif du scan.

BATCH 2 · IP-GPS-002A / 002B / 002C

IP ANALYZER

IP GLOBAL ASSESSMENT — 3.72.171.177 LIVE

IP Global Assessment — le premier résultat spectaculaire

La vraie page. Les signaux qui comptent. Le résumé exécutif.

002A · Assessment Page

RISK
MEDIUM-HIGH

CONFIDENCE
86%

STATUS
ACTIVE

EVIDENCE QUALITY
HIGH

Identité rapide

- ASN / Operator: AS15169 · Example Net
- Country / region: NL · Amsterdam
- Profile: Cloud edge / hosting
- Last scan: 20 Sep 2026 · 09:14
- Execution time: 4.2s

002B · Signal Zones

GOOD REASSURING

- BGP origin consistent
- RPKI valid

NEEDS ATTENTION

- Unexpected exposed service
- Routing path changed

IMPORTANT

- Reputation source reported adverse evidence

• Uniquement les signaux réellement présents · chaque ligne est cliquable •

002C · What You Should Know

1. Origin BGP cohérente avec l'ASN annoncé
2. RPKI valide — pas de hijack obvious
3. Service inattendu exposé sur le périmètre
4. Changement récent de chemin de routage
5. Une source de réputation signale un indice adverse
6. Qualité de preuve élevée, confiance 86%

Le résumé exécutif du scan

002A page réelle • 002B zones Good • Attention • Important • 002C What You Should Know •

NEW IDEAS

TO DO LIST

- **STORE RESULT IN DATABASE - Done**
- **INTEGRATE IN DASHBOARD - Done**
- **MANAGE HISTORIC FOR IP ANALYZER - Done**
- INTEGRER UN PAGE « BILAN » QUI RESUME L ANALYSE DE L IP
- INTEGRER UN WIZARD/GPS (Comme avec security Analyzer)
- **IL FAUT INTEGRER UNE PROGRESS BAR + MESSAGES DURANT L ANALYSE - Done**
- SUR L IP ANALYZER IL FAUDRAIT UNE PAGE DE BILAN GLOBAL SUR L ANALYSE DE LIP (CE QUIL Y A DIMPORTANT RETENIR BON OU MAUVAIS), Cette Page pouvant être appellée de la Liste des IP analysées (Modal) ou Bien à partir d'un Gros bouton en tête de la page générale du DashBoard + RECOMMANDATIONS IMPORTANTES ou ACTIONS A FAIRE (S'il y en a bien sûr)
- FICHIER AIDE POUR EXPLIQUER QUELS ANALYZERS SONT LANCES + UNE MINI MODAL D EXPLICATION SUR CHACUN DE CES ANALYZER
- CREER UNE PAGE HISTORICAL INTELLIGENCE
- VERIFIER ENFIN QUE LE RESULTAT DE TOUS LES ANALYZER SONT BIEN PRESENTS DANS LE DASHBOARD
- **Outils de remise à zéro de l'Outils** (***demandée et exigée***)
- **Travailler sur la Remediation** , Problème identifiés, quelles action, Patch, commandes, ..

```
Analyzers
---------
ip-input              OK       0.021 ms
rdap                  OK       858.463 ms
  warning: RDAP alone does not confirm the current operator or BGP origin; routing analyzers correlate those signals later in the run.
asn                   OK       1529.664 ms
bgp                   OK       451.842 ms
rpki                  OK       80.662 ms
geo                   OK       219.676 ms
network-type          OK       0.082 ms
  warning: No network type reached the minimum evidence threshold.
geo-consensus         OK       0.126 ms
  warning: Geolocation providers disagree on one or more location fields.
reverse-dns           OK       4.12 ms
  warning: PTR name exists, but forward resolution did not return the original target address.
dns-association       OK       3.462 ms
passive-exposure      OK       21.403 ms
service-exposure      OK       0.054 ms
reputation-sources    OK       452.316 ms
abuse-signals         OK       0.072 ms
reputation-consensus OK       0.048 ms
  warning: Reputation consensus has fewer than two evaluable provider responses.
tls                   OK       2.488 ms
active-exposure       OK       3004.453 ms
  warning: TCP connect validation tests reachability only; it does not authenticate or exploit any service.
deep-trace            OK       27068.116 ms
  warning: ICMP ping sockets are not permitted for this user.
  warning: udp-paris did not receive a destination response within the hop limit.
  warning: udp-paris stopped at adaptive TTL 5 after another method reached the destination at TTL 2.
  warning: udp did not receive a destination response within the hop limit.
  warning: udp stopped at adaptive TTL 5 after another method reached the destination at TTL 2.
trace-hops            OK       474.865 ms
trace-consensus       OK       0.198 ms
  warning: Batch 8 is a single local-server vantage. Batch 9 performs multi-vantage comparison.
evidence-fusion       OK       0.26 ms
coherence-engine      OK       0.055 ms
  warning: Geolocation providers disagree
correlation-engine    OK       0.273 ms
  warning: Correlation engine retained 1 unresolved contradiction(s).
historical-intelligence OK       5.172 ms
```

```
Historical Intelligence
-----------------------
Status             : OK
Mode               : changed
Snapshots          : 10
Snapshot ID        : 12
Previous ID        : 11
First seen         : 2026-09-17T13:25:28.089838+00:00
Previous seen      : 2026-09-19T13:51:27.307987+00:00
Material changes   : 1
Coverage changes   : 0
Highest severity   : low
Risk delta         : 0.0
Confidence delta   : 0.0
Risk trend         : stable
Confidence trend   : stable
Changed sections   : trace
  CHANGE [LOW] Trace path fingerprint
    5df205eee193124122e26b06a49a4e556e93e0c96f78a4a575ba5c633d8f5a4a -> e5e5e780547a0d51c835e29a84324f62836ed3aef3cb82de75c404ac345f75a3
```

Ce qui manque vraiment : passer de « cette IP » à « cet écosystème »

Aujourd'hui l'unité d'analyse est **une adresse**. Les enquêtes poussées gagnent surtout quand on élargit à :

- le **préfixe** et les voisins
- le **certificat / domaine**
- l'**ASN / politique de routage**
- le **temps** (première apparition, rotation, hijack)
- le **graphe** de partage d'infra

C'est là que se trouvent les plus gros gains.

AGENDA NOUVELLES FONCTIONS

- 1. Intelligence de voisinage de préfixe IP-INTEL-015A
- 2. Graphe d'infrastructure partagée
- 3. Passive DNS + Certificate Transparency historiques
- 4. Empreinte applicative bornée
- 5. Classification cloud / CDN / anycast / POP
- 6. PeeringDB + facility + IX
- 7. Hygiène de routage de l'ASN, pas seulement de l'IP
- 8. Jumeau IPv6 / dual-stack
- 9. Rôle métier du host IP-INTEL-015B
- 10. Couche renseignement élargie, toujours conservative
- 11. Déjà dans vos données : 4 moteurs « zéro réseau »

1. Intelligence de voisinage de préfixe — `IP-INTEL-015`

Idée. Une IP isolée ment souvent. Un `/24`, un more-specific, ou les 8–16 voisins racontent le vrai métier du bloc.

Analyses possibles (passives d'abord) :

- densité de services sur le préfixe annoncé (via InternetDB / CT / PTR déjà en cache)
- ratio hosting / résidentiel / scanner / sinkhole dans le voisinage
- PTR homogènes (`ec2-…compute.amazonaws.com`) vs PTR « bricolés »
- même certificat, même favicon hash, même titre HTTP sur plusieurs IPs du bloc
- verdict : *hôte dédié*, *parking mutualisé*, *bloc freshly allocated*, *plage d'abuse*

Sur votre exemple `3.72.171.177` / `3.64.0.0/12` AMAZON-FRA, le voisinage confirmerait immédiatement « compute AWS eu-central-1 » plutôt qu'un site standalone.

Valeur enquête. Distingue un serveur unique d'une ferme, d'un CDN anycast, ou d'un préfixe « jetable ».

IP-INTEL-015A — Prefix Neighborhood

Objectif

Répondre à : *cette IP est-elle un hôte isolé, une maille cloud, un bloc mutualisé, ou une plage d'abuse ?*

Périmètre du voisinage

Priorité, du plus précis au plus large :

1. préfixe **BGP annoncé** (`asn.prefix` / `bgp.prefix`) s'il est `≤ /24` IPv4 ou `≤ /48` IPv6
2. sinon le `/24` IPv4 contenant la cible (ou `/64` IPv6, jamais plus large)
3. jamais le `/12` Amazon entier

Sur `3.72.171.177` , le préfixe routé est `3.64.0.0/12` → **trop large**. On tombe sur le `/24` `3.72.171.0/24` . C'est une règle dure : si le préfixe annoncé a plus de **256** adresses IPv4 (ou 256 slots » IPv6 échantillonnés), on échantillonne.

Échantillonnage borné :

- cible + `±1..7` dans le `/24` (15 IPs max par défaut)
- env `IP_INTEL_NEIGHBOR_SAMPLE=15` (min 5, max 32)
- jamais de TCP connect, jamais de traceroute voisin

Sources autorisées (passives)

Réutiliser uniquement des collecteurs **déjà payés** dans le run, plus un cache local :

Source	Usage
PTR système / `reverse-dns`	motif de nommage du voisin
InternetDB déjà utilisée par `passive-exposure`	ports / hostnames / CPE du voisin
snapshot historique local si le voisin a déjà été scanné par ce workspace	rôle / risque antérieur
pas RDAP/BGP/RPKI par voisin	trop cher, redondant

Si InternetDB n'a rien pour un voisin : le voisin compte comme `unobserved`, pas comme `clean`.

Données de sortie

text Copier

```
analyzer: prefix-neighborhood
status: success | partial | skipped
```

Champs utiles :

- `scope.prefix` — ex. `3.72.171.0/24`
- `scope.reason` — `announced-prefix` | `fallback-slash24` | `sampled-large-prefix`
- `sample_size`, `observed_count`, `unobserved_count`
- `naming.pattern` — regex/token dominant (`ec2-*-eu-central-1.compute.amazonaws.com`)
- `naming.homogeneity_percent`
- `exposure.port_union`, `shared_product_ratio`
- `sibling_hostnames` — hostnames InternetDB/PTR qui ne sont pas la cible
- `verdict` :
  - `homogeneous-cloud-block`
  - `homogeneous-hosting-block`
  - `mixed-shared-block`
  - `sparse-or-dedicated`
  - `insufficient-neighborhood`
- `confidence_percent`
- `warnings[]`

Heuristiques (explicables, pas un ML opaque)

Exemples de règles, chacune productrice d'evidence :

- `≥ 70%` des PTR observés partagent le même motif cloud → +40 vers `homogeneous-cloud-block`
- même produit (`f5/nginx` , `openssh`) sur `≥ 50%` des voisins observés → +15 shared-infra
- ports très hétérogènes + PTR hétérogènes → `mixed-shared-block`
- `observed_count < 3` → verdict `insufficient-neighborhood` , confiance plafonnée à 45

Ce que 015A ne fait pas

- pas de scan des 256 adresses
- pas d'inférence « le voisin est malveillant donc la cible l'est »
- pas de géoloc par voisin (quota)

Prefix neighborhood intelligence

IP-INTEL-015

An isolated IP often lies — the /24, more-specific, or 8–16 neighbors reveal the block's real job.

3.72.171.177

Announced prefix: 3.64.0.0/12

AMAZON-FRA

Neighbors ±8 on 3.72.171.0/24

Passive sources: InternetDB · CT · PTR cache

Compute farm — AWS eu-central-1

~~Not a standalone site~~

Dedicated host No | Shared parking No | Freshly allocated No | Abuse range No

Service density
72%
of sampled IPs have open services

Hosting / cloud ratio
94%

PTR homogeneity
High

Shared artifacts
11/16
neighbors share cert or title pattern

Neighborhood composition



Hosting/cloud 94% · Scanner 3% · Residential 1% · Sinkhole 2%

Ratio hosting / residential / scanner / sinkhole

PTR pattern

- ec2-3-72-171-177.eu-central-1.compute.amazonaws.com (target)
- ec2-3-72-171-176.eu-central-1.compute.amazonaws.com
- ec2-3-72-171-178.eu-central-1.compute.amazonaws.com
- ec2-3-72-171-180.eu-central-1.compute.amazonaws.com

Homogeneous PTR (ec2-*.compute.amazonaws.com) vs handmade PTR — verdict: cloud inventory, not boutique host.

Neighbor strip

IP	PTR class	Services	Shared cert	Shared title
3.72.171.170	ec2 AWS	22,443	yes	—
3.72.171.173	ec2 AWS	443	yes	—
3.72.171.176	ec2 AWS	80,443	yes	default
3.72.171.177	ec2 AWS TARGET	22,80,443	yes	—
3.72.171.178	ec2 AWS	443	yes	—
3.72.171.181	ec2 AWS	22	yes	—
3.72.171.184	scanner-like	22	no	—
3.72.171.185	ec2 AWS	443	yes	—

Investigation value: distinguishes a unique server from a compute farm, anycast CDN, or disposable prefix. Here the block behaves like AWS compute eu-central-1.

2. Graphe d’infrastructure partagée — `IP-INTEL-016`

Idée. Construire un petit graphe à partir de ce que vous avez déjà, plus 2–3 sources :

`IP → prefix → ASN → PTR → domaines DNS → certificats TLS → autres IPs`

Pivots utiles :

- même serial / fingerprint SHA-256 de certificat
- mêmes SAN
- mêmes NS / SOA
- même titre + hash favicon (Shodan-style, passif)
- même path signature de traceroute (déjà calculée)
- mêmes upstreams BGP

Le Batch 13C « IP A vs IP B » devient alors un cas particulier d’un **cluster**. Sortie : « 14 IPs, 3 domaines, 1 cert Let’s Encrypt, 1 ASN, 1 POP Francfort ».

Valeur enquête. C’est le vrai mode investigation, pas seulement un score.

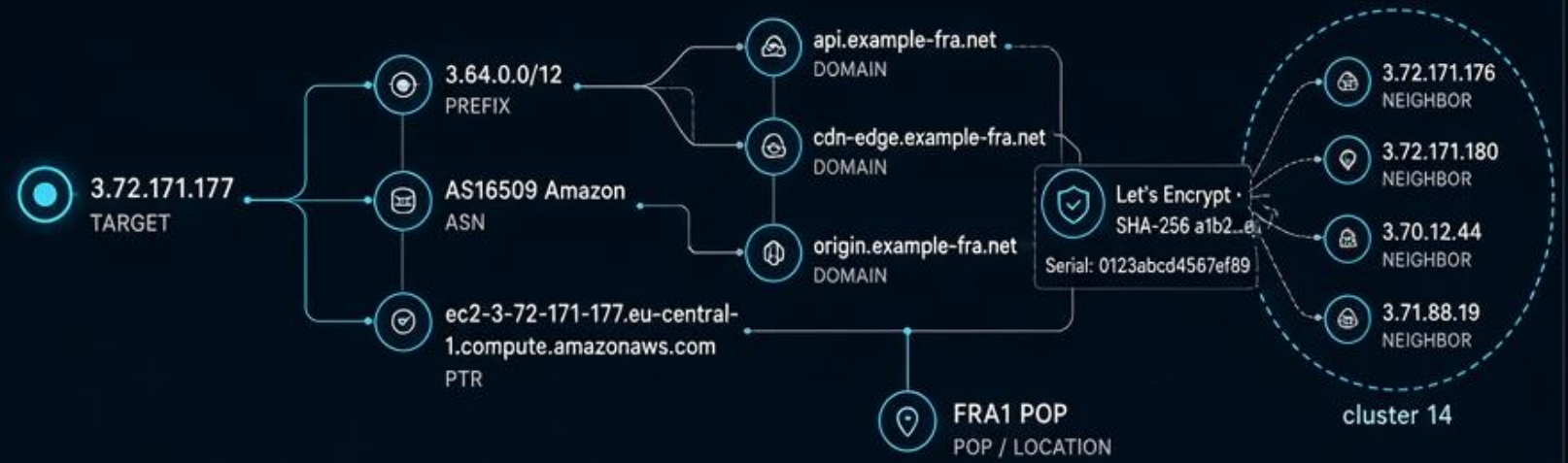
Shared infrastructure graph

IP-INTEL-016

IP → prefix → ASN → PTR → DNS domains → TLS certs → other IPs. Investigation mode, not a score.

14 IPs | 3 domains | 1 Let's Encrypt cert | 1 ASN (AS16509) | 1 Frankfurt POP

Seed IP highlighted: 3.72.171.177 · prefix 3.64.0.0/12 AMAZON-FRA



Pivots used

- ✓ Same cert serial SHA-256
- ✓ Same SANs
- ✓ Same NS / SOA
- ✓ Same HTTP title + favicon hash (passive)
- ✓ Same traceroute path signature
- ✓ Same BGP upstreams

Cluster members

IP	Role	Pivot
3.72.171.177	seed	—
3.72.171.176	neighbor	cert + PTR
3.72.171.180	neighbor	cert + SAN
3.70.12.44	same cert	SHA-256
3.71.88.19	same NS/SOA	dns

ⓘ Note: Batch 13C IP A vs IP B is a 2-node special case of this cluster.

ⓘ Output: 14 IPs, 3 domains, 1 Let's Encrypt cert, 1 ASN, 1 Frankfurt POP — shared infrastructure, not an isolated host.

3. Passive DNS + Certificate Transparency historiques — `IP-INTEL-017`

Vous avez le TLS **actuel** de l'IP et quelques noms associés (`www.ideo-lab.com`). Il manque l'axe temps.

- **CT logs** : tous les certificats jamais émis pour les domaines vus, explosion de SAN, wildcards, réémissions fréquentes
- **Passive DNS** (CIRCL, Farsight, VT, SecurityTrails…) : domaines qui ont **pointé** vers cette IP, dates first/last seen
- détection **fast-flux** : beaucoup de domaines courts, TTL bas, rotation d'IPs
- divergence DNS actuel vs historique (domaine légitime qui a quitté l'IP, ou l'inverse)

Valeur enquête. Une IP « propre » aujourd'hui peut être un ancien C2, un parking, ou un hôte qui a changé 40 fois de sites.

Historical Passive DNS + CT

Current TLS is one point in time. CT logs and passive DNS restore the time axis.

IP 3.72.171.177 · AS16509 · AMAZON-FRA

Current name

www.ideo-lab.com

Current cert: Let's Encrypt, expires 2026-12-04

Fast-flux: No

Current vs history: Divergence
IP reused; current name is recent on this address

Host churn: 40 prior names on this IP
(cloud reuse pattern)

Not labeled malware; verdict Clean today · historically shared cloud IP

PDNS names	CT certs for seen domains	Wildcard / SAN explosion	Reissues
41	18	Low	6 (Let's Encrypt 90-day)

Timeline: Historical occupancy and certificate events



Passive DNS

Name	First seen	Last seen	Source
www.ideo-lab.com	2025-04-11	2026-09-19	CIRCL / SecurityTrails
mail.ideo-lab.com	2025-04-12	2026-09-19	Farsight
api.ideo-lab.com	2025-06-02	2026-08-30	VT
legacy-tenant-a.net	2023-01-08	2024-11-02	CIRCL
cdn-edge-old.example	2022-09-14	2023-03-21	Farsight

Sources: CIRCL · Farsight · VT · SecurityTrails

Certificate Transparency

2026-09 — Let's Encrypt
CN=www.ideo-lab.com
SAN: ideo-lab.com, www.ideo-lab.com

2026-06 — Let's Encrypt reissue
CN=www.ideo-lab.com
SAN: ideo-lab.com, www.ideo-lab.com

2025-04 — First issuance (Let's Encrypt)
CN=www.ideo-lab.com
SAN: ideo-lab.com, mail.ideo-lab.com

Note: no SAN explosion, no unexpected wildcards.

Investigation value: a clean IP today can be an old C2, parking, or a host that changed sites 40 times. Here: reused AWS IP; ideo-lab.com is the current tenant, not the only historical occupant.

4. Empreinte applicative bornée — `IP-INTEL-018` (profil `deep` + `--active`)

Vous validez déjà TCP 80/443 et lisez le certificat. On peut aller plus loin **sans exploit** :

Signal	Ce qu'il apporte
Chaîne de redirects HTTP	CDN / WAF / origin vs page parking
En-têtes `Server`, `Via`, `CF-Ray`, `x-amz-cf-id`, `X-Cache`	Cloudflare, CloudFront, Akamai, nginx/F5 déjà vu
ALPN / HTTP/2 SETTINGS / JARM / JA4	famille de stack, pas seulement « port ouvert »
QUIC (UDP 443)	front CDN moderne vs origine nue
Favicon mmh3 + `<title>`	jumeaux d'infra
Banner SSH/SMTP **en lecture seule**	rôle réel du host (mail, jump, web)

Garder le même garde-fou que `active-exposure` : connect only, timeout court, liste de ports bornée, aucun payload d'exploitation.

Valeur enquête. Sur votre trace, `f5/nginx` + Let's Encrypt + `www.ideo-lab.com` : on saurait si c'est un reverse-proxy AWS, un origin, ou un WAF devant un autre ASN.

Bounded application fingerprint

IP-INTEL-018 | deep + active

Go past open 80/443 and the cert — connect-only, short timeout, bounded ports, no exploit payload.

Target: www.ideo-lab.com

3.72.171.177 · AS16509 · AMAZON-FRA

Ports probed 80 443 22 25 only

AWS reverse-proxy / origin on AS16509

- Not a third-party WAF in front of another ASN
- Not CloudFront / Cloudflare / Akamai
- Stack: F5/nginx + Let's Encrypt
- Guardrail: active-exposure · connect-only

1 HTTP redirect chain

Observed

80 → 301 https://www.ideo-lab.com/ → 200

Meaning:
origin / reverse-proxy, not parking page

2 Headers

Observed
Server: nginx
Via: 1.1 varnish-like empty or "—"
CF-Ray: absent
x-amz-of-id: absent
X-Cache: absent

Meaning:
no Cloudflare / CloudFront / Akamai in front

3 ALPN / H2 / JARM / JA4

Observed
ALPN: h2, http/1.1
HTTP/2 SETTINGS present
JARM: 29d29d... (short)
JA4: t13d... (short)

Meaning:
stack family nginx/F5, not just "port open".

4 QUIC UDP/443

Observed
Not offered

Meaning:
not a modern CDN front; closer to naked origin or classic reverse-proxy.

5 Favicon mmh3 + title

Observed
title: "IDEO Lab",
mmh3: 123456789,
Twins: 2 hosts same hash in neighborhood

Meaning:
infra twins

6 SSH / SMTP banners read-only

Observed
22: closed
25: closed

Meaning:
web role, not mail or jump host.

Guardrail = active-exposure: connect only · timeout 3s · ports {80,443,22,25} · no exploit payload

Insight: f5/nginx + Let's Encrypt + www.ideo-lab.com on AS16509 → reverse-proxy/origin on AWS, not a WAF fronting a different ASN.

5. Classification cloud / CDN / anycast / POP — `IP-INTEL-019`

Le `network-type` est aujourd'hui `unknown / 0%` alors que les signaux sont déjà là :

- motif PTR `ec2-3-72-171-177.eu-central-1.compute.amazonaws.com`
- AS16509 + NetName `AMAZON-FRA`
- RTT destination ~0,2 ms depuis un vantage trop proche, ou géométrie multi-vantage
- en-têtes cloud / anycast

Moteur dédié :

1. parseurs de nommage AWS / GCP / Azure / Oracle / Hetzner / OVH
2. tables de préfixes cloud (public ranges)
3. heuristique anycast : même IP, RTT incompatibles entre vantages (vous avez déjà les latency envelopes)
4. hypothèse de **région / AZ / facility**, pas d'adresse postale

Sortie : `cloud=AWS`, `product=EC2`, `region=eu-central-1`, `anycast=no`, `confidence=93%`.

C'est exactement le trou visible sur le run `3.72.171.177`.

Cloud / CDN / anycast / POP

IP-INTEL-019

network-type was unknown / 0% — the signals were already there.

IP	3.72.171.177
PTR mono:	ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
AS16509 · NetName	AMAZON-FRA
RTT dest	~0.184 ms (single nearby vantage)

OUTPUT – CLASSIFICATION RESULT

cloud	AWS
product	EC2
region	eu-central-1
anycast	no
confidence	93%

Replaces old field *"network type: unknown"*

ENGINE STEP BREAKDOWN

1 Naming parsers
AWS PTR matched,
(also lists GCP / Azure / Oracle / Hetzner / OVH as supported)

2 Cloud prefix tables
3.64.0.0/12 in AWS public ranges.

3 Anycast heuristic
no incompatible RTT across vantages.
(0 successful extra vantages; single-probe RTT 0.18ms is proximity, not anycast).

4 Region / AZ / facility hypothesis
eu-central-1 inferred from PTR, not a postal address.

SIGNALS USED

PTR motif	EC2 eu-central-1
ASN + NetName	AMAZON-FRA
Destination RTT	~0.2 ms from nearby vantage
No CDN anycast headers	(no CF-Ray, no x-amz-cid-id)
	(no CF-Ray, no x-amz-cid-id)

FACILITY HYPOTHESIS

Frankfurt / eu-central-1
facility hypothesis

not a street address



INSIGHT This is the exact hole on run 3.72.171.177: type unknown while AWS EC2 eu-central-1 was readable from PTR + prefix + ASN.

6. PeeringDB + facility + IX — `IP-INTEL-020`

Le traceroute enrichit ASN/geo des hops, mais pas la **salle**.

Sources passives : PeeringDB, RIPEstat, heuristiques de noms (`eqix-fr5`, `interxion`, `de-cix`).

Pour chaque hop public :

- IX vs transit vs last-mile
- facility probable (Equinix FR5, Interxion FRA, DE-CIX…)
- distance facility → consensus geo de la cible

Valeur enquête. « L'IP est en Allemagne » devient « last hop dans un campus Equinix Francfort, cohérent avec AWS FRA ». Beaucoup plus actionnable, toujours au niveau infrastructure.

PeeringDB + facility + IX

Traceroute already has ASN/geo per hop. This page adds the room — the facility.

Last hop on Equinix Frankfurt campus, coherent with AWS FRA

not merely "the IP is in Germany"

Target 3.72.171.177 · AS16509 · AMAZON-FRA · geo consensus Frankfurt am Main

Distance facility → geo consensus: < 15 km · consistent

Sources: PeeringDB | RIPEstat | name heuristics (eqix-fr5, interxion, de-cix)

HOP FACILITY TABLE (2-HOP TRACE)

1 Hop 1 · 244.5.0.111	Role: not a public hop	IX/transit/last-mile: —	Facility: not applicable	Note: reserved 240/4, vantage/internal artifact	
2 Hop 2 · TARGET · 3.72.171.177	Role: last-mile / cloud edge	IX vs transit vs last-mile: last-mile (cloud)	Probable facility: Equinix FR5 / Frankfurt campus	Also listed: Interxion FRA presence, DE-CIX Frankfurt IX (peering, not the compute hall)	Distance to geo consensus: 8 km · coherent

FRANKFURT FACILITY MAP (SCHEMATIC)



facility hypothesis, not a postal address

PEERING CONTEXT

- AS16509 present at DE-CIX Frankfurt (PeeringDB)
- No eqix-fr5 / interxion / de-cix token in this hop hostname (EC2 PTR instead)
- Inference from prefix + ASN + PeeringDB facility set, not from hop rDNS

Investigation value: 'IP is in Germany' becomes 'last hop in an Equinix Frankfurt campus, coherent with AWS FRA'. Actionable at infrastructure level.

7. Hygiène de routage de l'ASN, pas seulement de l'IP — `IP-INTEL-021`

Vous validez RPKI et l'origine BGP de **ce** préfixe. Un enquêteur regarde l'opérateur :

- IRR (RIPE/RADB) vs origine **live**
- first-seen BGP du préfixe (RIPEstat)
- âge d'allocation RDAP vs première annonce
- MOAS, more-specific soudain, AS-PATH bizarre
- score ManRS / présence dans listes « bulletproof »
- volume d'abuse **au niveau ASN** (pas seulement l'IP)

Signaux forts pour la fraude : préfixe annoncé depuis 48 h, RPKI valid mais IRR vide, upstream inhabituel.

L'historique Batch 11 stocke déjà `path_signature` et `origin_asns` : il « suffit » d'y ajouter first-seen + IRR.

ASN routing hygiene — not just the IP

RPKI and BGP origin of this prefix are already known. An investigator looks at the operator.

Prefix 3.64.0.0/12

Origin AS16509 · AMAZON-02 · Amazon.com, Inc.

RPKI VALID · origin consistent · multi-origin no

Batch 11 already stored: path_signature + origin_asns

Routing hygiene: HEALTHY

Fraud pattern: not matched

Not "announced 48h + RPKI valid + empty IRR + unusual upstream"

Confidence 96%

1 IRR vs live origin

RIPE/RADB route objects for 3.64.0.0/12 originate AS16509
Live BGP origin AS16509

Status MATCH

2 BGP first-seen (RIPEstat)

Prefix first announced 2017-12-18 (example long-lived AWS)
Age: ~9 years · not 48 hours

Status MATCH

3 RDAP allocation vs first announce

Allocation age older than first BGP visibility
No newborn prefix

Status MATCH

4 MOAS / more-specific / AS-PATH

MOAS: no
Sudden more-specific: none observed
AS-PATH: AS16509 origin only, no bizarre prepend/ odd transit

5 ManRS / bulletproof lists

ManRS: participant
Bulletproof hosting lists: absent

Status MATCH

6 Abuse volume at ASN level

AS16509 volume high as expected for hyperscaler
Not treated as bulletproof ASN; IP-level abuse still separate.

Strong fraud tells (not this case) → prefix announced 48h · RPKI valid but IRR empty · unusual upstream

Valid RPKI on a 48-hour prefix with empty IRR is a hijack/fraud tell. Here IRR matches live origin and the prefix is long-lived AWS.

8. Jumeau IPv6 / dual-stack — `IP-INTEL-022`

Pour une IPv4 :

- AAAA des domaines associés
- PTR IPv6 du même motif
- même certificat sur l'IPv6
- même last-hop ASN

Souvent l'IPv6 est moins durcie, moins listée, et révèle d'autres services. Inversement, une IPv6 seule doit chercher son IPv4 jumelle.

IPv6 twin / dual-stack

For an IPv4: AAAA of associated names, IPv6 PTR of the same motif, same cert, same last-hop ASN. IPv6 is often less hardened and less listed.

IPv4 seed

3.72.171.177

PTR: ec2-3-72-171-177.eu-central-1.compute.amazonaws.com

AS16509 · Amazon · eu-central-1

www.ideo-lab.com A record

TWIN

✓ AAAA ✓ Cert
✓ PTR motif ✓ ASN

IPv6 twin

2a05:d014:9c2:8a00:0:0:0:177

PTR: ec2-177.eu-central-1.compute.amazonaws.com (same motif)

AS16509 · same last-hop ASN

www.ideo-lab.com AAAA record Match confidence 91%

1 AAAA of associated domains

www.ideo-lab.com → 2a05:d014:9c2:8a00::177
mail.ideo-lab.com → same IPv6
api.ideo-lab.com → same IPv6

2 IPv6 PTR same motif

ec2-*.eu-central-1.compute.amazonaws.com
aligned with IPv4 PTR pattern

3 Same certificate on IPv6

Let's Encrypt CN=www.ideo-lab.com
SHA-256 match with IPv4:443
SANs identical

4 Same last-hop ASN

Trace IPv6 last hop AS16509
Matches IPv4 hop 2

Exposure delta: IPv6 open services vs IPv4

443 open both · 80 open both · 22 closed IPv4 · 22 OPEN on IPv6 ⚠
25 closed both

Not on major blocklists (IPv6 less listed)

Inverse search note: A lone IPv6 must search its IPv4 twin — this page runs both directions.

Insight: Dual-stack twin found on AWS eu-central-1. Same tenant, same cert, same ASN. IPv6 exposes SSH that IPv4 does not.

9. Rôle métier du host — `IP-INTEL-023`

Au lieu de « ports 80/443 ouverts », un classifieur de **fonction** :

- origin web / reverse-proxy / CDN edge
- MX / submission
- resolver DNS (ouvert ou non)
- VPN concentrator
- nœud Tor / proxy résidentiel
- scanner / honeypot / sinkhole
- API cloud / load-balancer

Entrées : ports + produits Shodan + bannières + TLS CN + PTR + GreyNoise classification + geo/network-type.

Sortie lisible pour le « bilan global » déjà noté dans le PDF page 204.

IP-INTEL-015B — Host Role Classifier

Objectif

Remplacer `network-type: unknown 0%` par un **rôle d'infrastructure** à partir des analyseurs déjà exécutés. C'est le correctif le plus visible du produit.

Taxonomie (une primaire + flags)

Rôle primaire (`primary_role`) :

Rôle	Signaux typiques
`cloud-compute`	PTR EC2/GCE/Azure, ASN cloud, NetName région
`cloud-lb-or-edge`	PTR `elb` , `cloudfront` , `azure-trafficmanager`
`cdn-anycast`	AS Cloudflare/Akamai/Fastly + géométrie RTT incompatible
`datacenter-hosting`	hosting ASN, PTR générique hébergeur
`reverse-proxy`	nginx/f5 + un seul vhost TLS ≠ PTR
`mail-mta`	25/587/465, PTR `mail
`dns-resolver`	53 observé, PTR `ns|dns`
`vpn-or-proxy`	flags network-type + ports 1194/51820/443-only atypique
`tor-exit`	listes / flags déjà présents
`scanner-or-noise`	GreyNoise noise sans service utile
`sinkhole-or-honeypot`	RIOT/benign infra connue
`residential-or-cgnat`	flags mobile/residential, ASN opérateur

Flags booléens séparés (cumulables) : `virtual_hosted`, `cdn_fronted`, `anycast_suspected`, `dual_name_ptr_tls`.

Entrées (lecture seule des `results`)

- `rdap` : netname, org, owner vs operator
- `asn` / `bgp` : holder, prefix size, origin
- `network-type` : flags existants (vpn/proxy/tor/hosting/mobile…)
- `reverse-dns` + `dns-association`
- `tls` : CN/SAN vs PTR
- `passive-exposure` + `service-exposure` + `active-exposure`
- `reputation-consensus` + GreyNoise natif
- `trace-consensus` / `multi-vantage-consensus` : RTT spread, path
- `prefix-neighborhood` : homogénéité du bloc

Parseurs de nommage (prioritaires, déterministes)

Table initiale, standard-library, testable :

Motif PTR / hostname	Rôle	Produit	Région extraite
`ec2-*.*.compute.amazonaws.com`	`cloud-compute`	`AWS-EC2`	`eu-central-1`
`*.elb.amazonaws.com`	`cloud-lb-or-edge`	`AWS-ELB`	groupe
`*.cloudfront.net`	`cdn-anycast`	`AWS-CloudFront`	—
`*.googleusercontent.com`	`cloud-compute`	`GCP`	—
`*.cloudapp.azure.com`	`cloud-compute`	`Azure`	—
`*.hetzner.com` / `*.ovh.net`	`datacenter-hosting`	vendor	—

Sur le run réel :

```text
PTR = ec2-3-72-171-177.eu-central-1.compute.amazonaws.com
NetName = AMAZON-FRA
Operator = AMAZON-02 / AS16509
```

→ `primary_role=cloud-compute`, `product=AWS-EC2`, `region_hint=eu-central-1`, `facility_hint=AWS-FRA`, confiance ≥ **90** même si `network-type` reste unknown.

Réinterprétation des observations Batch 10

015B doit émettre des **resolutions**, pas cacher les contradictions :

Code actuel	Si rôle cloud + virtual host	Nouveau traitement
`NETWORK_TYPE_UNRESOLVED`	rôle trouvé par PTR/ASN	`ROLE_RESOLVED_FROM_INFRA_SIGNALS` (agreement)
`DNS_TLS_NAME_DIVERGENCE`	SAN `ideo-lab.com` vs PTR AWS	`CLOUD_VIRTUAL_HOSTING` (observation légitime)
`PTR_FORWARD_MISMATCH`	forward → `172.31.42.227` (RFC1918)	`PROVIDER_INTERNAL_FORWARD_ZONE` (attendu AWS)
`GEO_PROVIDER_DISAGREEMENT`	tous DE / Frankfurt ±2 km	rétrograder en observation basse si spread < 10 km

Sortie

```text
primary_role
role_confidence_percent
product             # AWS-EC2
region_hint         # eu-central-1
facility_hint       # AWS-FRA | Equinix-FR5 | unknown
virtual_hosted      # true
anycast_suspected   # false
naming_evidence[]   # list of matched patterns
overrides[]         # what we reinterpreted and why
candidates[]        # role=score like network-type
```

Seuil : si le meilleur score < 40 → `unknown` (pas de faux cloud).

Lien avec `network-type` existant

Ne pas jeter 004B. 015B **enrichit** :

```text
network-type.primary_type reste la source brute
host-role.primary_role est la classification opérationnelle
```

Le dashboard affiche `host-role`. Le CLI peut montrer les deux lignes.

Host business role

Not 'ports 80/443 open" — a function classifier for the bilan global.

3.72.171.177 · www.ideo-lab.com

AS16509 · EC2 eu-central-1 · AMAZON-FRA

PTR ec2-3-72-171-177.eu-central-1.compute.amazonaws.com

BILAN GLOBAL OUTPUT

PRIMARY ROLE: Origin web / reverse-proxy

SECONDARY: possible API front

NOT: CDN edge · MX · resolver · VPN · Tor · scanner/honeypot/sinkhole · cloud LB

Confidence **88%**

One-line bilan:
"Web origin / reverse-proxy on AWS EC2 FRA (nginx/F5 + Let's Encrypt), not a mail/VPN/Tor/scanner node."

ROLE SCORE LIST

Origin web / reverse-proxy	88%	SELECTED	
API cloud / load-balancer	24%	weak	
CDN edge	4%	rejected	(no CF-Ray / x-amz-of-id / QUIC)
MX / submission	1%	rejected	(25 closed, no MX banner)
Resolver DNS	2%	rejected	(53 closed)
VPN concentrator	1%	rejected	(no 1194/500/4500/51820)
Tor node / residential proxy	0%	rejected	
Scanner / honeypot / sinkhole	3%	rejected	(GreyNoise: not seen as scanner)

INPUTS USED

- Ports 80/443 open, 22/25/53 closed
- Shodan product: nginx
- Banners: nginx, no SSH/SMTP
- TLS CN: www.ideo-lab.com
- PTR: EC2 compute
- GreyNoise: unclassified / not noisy
- geo/network-type: AWS EC2 eu-central-1 (IP-INTEL-019)

INSIGHT Same host can be 'open 443' and still be mail, VPN, Tor, or a sinkhole. Role is the field the bilan global should print.

10. Couche renseignement élargie, toujours conservative — `IP-INTEL-024`

Vous avez GreyNoise Community, AbuseIPDB, ThreatFox, Spamhaus DQS (3/4 souvent non configurés). Sans changer la doctrine « absence ≠ safe » :

- URLHaus / MalwareBazaar / OTX (IOC IP)
- VirusTotal **passif** (résolutions, samples qui contactent l'IP)
- listes Tor exit, VPN commerciaux, proxies résidentiels
- sanctions / juridictions à risque (pays du consensus geo, pas la personne)
- réputation du **préfixe** et de l'**ASN**, séparée de celle de l'IP

Garder le modèle actuel : signaux adverse / rassurant / contextuel, couverture affichée, pas de verdict « safe ».

Expanded intel layer — still conservative

IP-INTEL-024

Absence of hits is not safety. Signals are adverse / reassuring / contextual. Coverage is shown. No 'safe' verdict.

IP 3.72.171.177 · prefix 3.64.0.0/12 · AS16509

absence ≠ safe

0 adverse hits on queried sources · 2 reassuring · 3 contextual · coverage 7/11 sources

ADVERSE

0 adverse hits on queried sources

GreyNoise Community	no scanner classification	✓ CLEAR
AbuseIPDB	0 reports (queried)	✓ CLEAR
ThreatFox	no IOC	✓ CLEAR
URLHaus	no URL on this IP	✓ CLEAR
MalwareBazaar	no sample	✓ CLEAR
OTX	no pulse	✓ CLEAR
VirusTotal passive	0 samples contacting IP (resolutions only to ideo-lab.com)	✓ CLEAR
Spamhaus DQS	NOT CONFIGURED	COVERAGE GAP

REASSURING

2 reassuring signals

- Not on Tor exit list
- Not on commercial VPN list
- Not on residential proxy list
- Geo jurisdiction DE: not a sanctioned country (country of consensus geo, not a person)

CONTEXTUAL

3 contextual signals

- AWS EC2 hyperscaler — ASN abuse volume expected, not attributed to this IP
- Prefix 3.64.0.0/12 reputation: cloud shared, do not inherit tenant guilt
- GreyNoise: unseen / unclassified ≠ benign

COVERAGE MATRIX

Queried threat intelligence coverage

CONFIGURED (7 SOURCES)

GreyNoise | AbuseIPDB | ThreatFox | URLHaus | MalwareBazaar | OTX | VT passive

NOT CONFIGURED (4 SOURCES)

Spamhaus DQS | Legacy Feed A | Legacy Feed B | Legacy Feed C

3/4 legacy feeds often unconfigured — shown as coverage holes

IP 3.72.171.177
no adverse IOC

Prefix 3.64.0.0/12
shared cloud, contextual only

ASN AS16509
high volume / hyperscaler context, not a verdict on this host

INSIGHT | Do not print SAFE. Print: no adverse IOC on covered sources; shared AWS prefix; DE geo not a sanctions hit; Spamhaus DQS uncovered.

11. Déjà dans vos données : 4 moteurs « zéro réseau »

Très rentables, alignés Batch 10 (pas de re-fetch) :

1. **Narratif + actions** (TODO page 204)
   « AWS EC2 Francfort, TLS ideo-lab.com, 0/100 risque, 1 contradiction geo, PTR non forward-confirmé. Actions : vérifier le nom virtuel, ne pas traiter la geo comme une adresse, surveiller le fingerprint de trace. »
2. **Détecteur de contradiction enrichi**
   Owner RDAP `A100 ROW GmbH` vs opérateur `AMAZON-02` vs PTR AWS vs cert `ideo-lab.com` : ce n'est pas un bug, c'est un **pattern cloud + virtual host**. Aujourd'hui c'est une observation `DNS_TLS_NAME_DIVERGENCE` ; demain ce doit être une classe nommée `CLOUD_VIRTUAL_HOSTING`.
3. **Score d'incertitude géo calibré cloud**
   Radius 100 km + « infrastructure-level only » est juste, mais pour EC2 FRA on peut dire « région AWS, pas ville utile ».
4. **Similarité intra-historique**
   Deux scans du même IP avec path fingerprint différent (`e5e5e7…` → `9469f6b0…` dans votre run) : déjà un changement matériel. En faire une alerte « topologie changée » avec gravité.

Zero-network engines

Already in your data. No re-fetch. Output for bilan global (PDF p.204).

3.72.171.177 · www.ideo-lab.com · AS16509

1 · Narrative + actions

"AWS EC2 Francfort, TLS ideo-lab.com, 0/100 risque, 1 contradiction geo, PTR non forward-confirmé."

Vérifier le nom virtuel | Ne pas traiter la geo comme une adresse | Surveiller le fingerprint de trace

Risk
0/100
contextual, not safe

2 · Enriched contradiction detector

RDAP owner:	A100 ROW GmbH
Operator:	AMAZON-02
PTR:	AWS EC2
Cert:	ideo-lab.com
Classification:	CLOUD_VIRTUAL_HOSTING (named class)
Deprecated observation label:	DNS_TLS_NAME_DIVERGENCE
Note:	not a bug — cloud + virtual host pattern

3 · Cloud-calibrated geo uncertainty

Consensus city	Frankfurt am Main
Calibrated statement	AWS region eu-central-1 — not a useful city
Radius	100 km · infrastructure-level only
City field	(operationally unused)
Confidence	in region high in street/city low

4 · Intra-history similarity

⚠ TOPOLOGY CHANGED

Same IP, two scans
path fingerprint e5e5e7… → 9469f6b0…

Severity: material

Action: watch trace fingerprint (links to engine 1)



Four engines, zero packets. Narrative, contradiction class, geo calibration, history delta — this is the bilan the PDF should print.

Proposition d’ordre (après 13/14)

Batch	Focus	Effort	Impact enquête
15	Voisinage de préfixe + rôle métier + narrative	moyen	immédiat
16	Graphe d’infra + comparaison généralisée	moyen	très fort
17	CT + passive DNS historique	dépend des API	très fort
18	Empreinte HTTP/TLS/QUIC bornée	moyen, `--active`	fort
19	Cloud/CDN/anycast/POP	faible (beaucoup de signaux existent)	fort sur vos cas AWS
20	PeeringDB/facility + hygiène ASN/IRR /first-seen	moyen	fort routing/fraude
21	Dual-stack IPv6 + enrichissement TI	variable	complémentaire

IP-INTEL-015C — Analysis Briefing

Objectif

Le modal / page demandé dans le TODO :

> *ce qu'il y a d'important à retenir (bon / mauvais) + recommandations / actions s'il y en a*

Pas un dump des 25 analyseurs. Un **briefing de 8 à 12 lignes**, déterministe.

Contrat de sortie

text Copier

```
analyzer: analysis-briefing
headline          # 1 phrase
posture           # favorable | mixed | attention | adverse
posture_reason
takeaways[]       # max 6, chacun {tone, text, sources[]}
actions[]         # max 5, chacun {priority, title, detail, optional}
non_actions[]     # ce qu'il ne faut PAS conclure
limitations[]     # repris / filtrés de correlation
```

`posture` n'est **pas** le risk score. Une IP AWS propre avec contradiction geo mineure = `favorable` ou `mixed`, risk 0/100.

Règle de posture :

Condition	Posture
risk ≥ 60 ou RPKI INVALID ou rôle `scanner-or-noise` adverse	`adverse`
risk 35–59 ou contradiction high restante	`attention`

Générateur de takeaways (templates, pas de LLM)

Chaque takeaway est un template avec slots remplis depuis les `results`. Exemples pour `3.72.171.177` :

1. **Identité** — `tone=info`
   « Compute AWS EC2, région `eu-central-1` / NetName `AMAZON-FRA`. Owner RDAP `A100 ROW GmbH` ≠ opérateur `Amazon.com, Inc.` : classique du cloud, pas un vol de préfixe. »
2. **Routage** — `tone=good`
   « Origine AS16509 cohérente, RPKI VALID. »
3. **Noms** — `tone=info`
   « PTR AWS interne ; certificat Let's Encrypt pour `www.ideo-lab.com`. Virtual hosting, pas une usurpation de nom par défaut. »
4. **Exposition** — `tone=info`
   « 80/443 ouverts, stack `f5/nginx`. Autres ports de la liste active non confirmés. »
5. **Réputation** — `tone=warn`
   « 0/100 mais couverture ~25 % (3 providers non configurés). Absence de signal ≠ IP sûre. »
6. **Chemin** — `tone=info`
   « Destination atteinte en 2 hops, vantage unique. Le fingerprint de trace a changé vs snapshot précédent : contexte réseau, pas preuve d'attribution. »

Actions (seulement si utiles)

Priorités : `now` | `review` | `optional`.

Catalogue fermé, pour ne pas inventer du bruit :

Code	Quand	Action
`CONFIGURE_REPUTATION_PROVIDERS`	coverage < 50 %	brancher AbuseIPDB / ThreatFox / Spamhaus DQS
`VERIFY_VIRTUAL_HOST`	`virtual_hosted`	vérifier que le vhost TLS est bien un site attendu du workspace
`DO_NOT_TREAT_GEO_AS_ADDRESS`	toujours si geo présent	geo = infra, pas domicile
`REVIEW_RPKI_OR_MOAS`	RPKI INVALID/MIXED ou origin inconsistent	revue routing
`REVIEW_NEW_PORTS`	`newly_observed_ports`	confirmer l'exposition nouvelle
`REVIEW_PATH_CHANGE`	historique `trace.path_signature` changed	noter un changement de chemin
`AUTHORIZE_TRACE_PROFILE`	profil quick et rôle encore `unknown`	proposer `--deep/--trace` si autorisé

S'il n'y a **aucune** action `now` / `review`, le briefing dit clairement « aucune action technique requise ; limitations de couverture seulement ».

`non_actions` (anti-surinterprétation)

Toujours générer 2–4 gardes-fous adaptés :

- « Ne pas conclure à une adresse physique à Francfort. »
- « Ne pas fusionner owner RDAP et opérateur BGP. »
- « Ne pas traiter un PTR privé `172.31.0.0/16` comme un mismatch hostile. »

C'est aligné slide 3 du PDF (caution MaxMind-style).

Intégration corrélation / cohérence / historique

Coherence (010B)

Nouveaux codes :

- agreement `ROLE_CLOUD_COMPUTE_CONVERGENCE`
- observation `CLOUD_VIRTUAL_HOSTING`
- observation `PROVIDER_INTERNAL_FORWARD_ZONE`
- observation `NEIGHBORHOOD_HOMOGENEOUS`
- observation `NEIGHBORHOOD_INSUFFICIENT`

Pénalité geo : si `host-role=cloud-compute` et spread < 10 km, `GEO_PROVIDER_DISAGREEMENT` passe de contradiction medium à observation low (le détail reste visible).

Correlation (010C)

- **Ne pas** augmenter le risk parce que c'est du cloud.
- **Augmenter la confiance** si rôle ≥ 85 % et routing cohérent (+5 cap 98).
- Ajouter dans `summary_points` la phrase de rôle en #1.
- Limitation dédiée si neighborhood `insufficient`.

History (011)

Ajouter dans `build_history_snapshot` une section `role` :

text Copier

```
observed
primary_role
product
region_hint
virtual_hosted
neighborhood_verdict
briefing_posture
```

Diff :

- changement de `primary_role` → **medium**
- changement de `briefing_posture` vers `adverse` → **high**
- changement de `region_hint` → **medium**
- neighborhood verdict only → **low**

C'est plus utile qu'un énième delta de ports.

CLI

Bloc court, après geo / avant exposure :

text Copier

```
Host role
---------
Primary role       : cloud-compute
Product            : AWS-EC2
Region hint        : eu-central-1
Virtual hosted     : yes
Neighborhood       : homogeneous-cloud-block (/24 sampled)
Confidence         : 93%

Analysis briefing
-----------------
Posture            : mixed
Headline           : AWS EC2 Francfort servant www.ideo-lab.com derrière nginx/F5.
  • AWS EC2 eu-central-1 ; owner RDAP ≠ opérateur Amazon (attendu).
  • RPKI VALID, origine AS16509 cohérente.
  • Réputation 0/100 à couverture 25%.
Actions
  - review  Configurer les providers de réputation manquants.
  - optional Vérifier que le vhost ideo-lab.com est le site attendu.
Non-conclusions
  - La geo Francfort n'est pas une adresse physique.
```

`--json` : les 3 analyseurs apparaissent dans `results[]` comme les autres.