

ICANN Domain Metrica

OCTO Security, Stability, and Resiliency Research

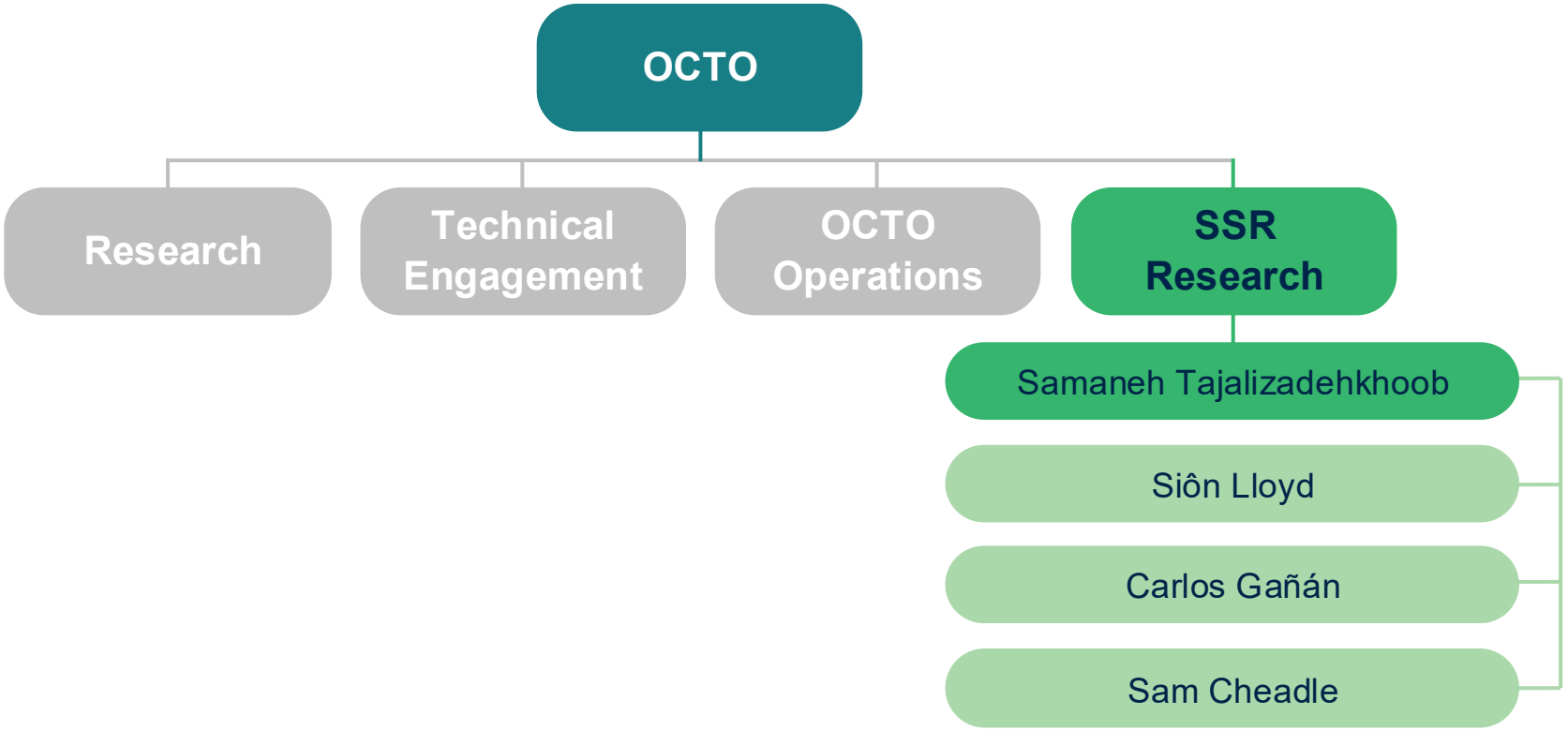
September 2026

Agenda

1. Meet the ICANN Domain Metrica Team
2. The Story Behind ICANN Domain Metrica
3. Deep Dive: Features & Benefits
4. Q&A

Meet the ICANN Domain Metrica Team

Our Team: Driving DNS Security Research



The Story Behind ICANN Domain Metrica

ICANN Domain Metrica: Your Comprehensive DNS Data Platform



Collects, combines, and compares DNS metadata



Dynamic dashboards, interactive visualizations



Flexible API for direct data access



Open and accessible for all ICANN account holders

- Global DNS trends for general users
- Customized views for registries and registrars

What Metrica is NOT



NOT for abuse investigation or attribution:

No threat hunting, forensics, or dispute adjudication.



NOT an abuse detection/ discovery tool:

Doesn’t crawl, scan or detect malicious activity.



Doesn’t take action against abusive domains:

No notifications, removals, or blocking.

How ICANN Domain Metrica Differs from Other Platforms

Diverse reputation data sources:
Integrates public and commercial RBLs for broad, balanced coverage.

Broad data integration:
Not just RBLs - DNS zones, registration data, popularity rankings, geolocation.

Dynamic and flexible:
Interactive dashboards, advanced filters, full API access.

Always evolving:
Designed for transparency and community-driven updates.

Granular analysis:
Search, filter, compare across domains, TLDs, and registrars.

User friendly:
Allows different users to interact in ways that suit them.

Goal: Empowering the Internet Community

Share ICANN's technical research

Consistent, impartial data on domain names



Enable open, trusted data for external research

Overcoming Abuse Metric Challenges

ICANN Domain Metrica addresses common pitfalls:

- Inconsistent DNS Abuse definitions
- Overlooked edge cases
- Registration lifecycle awareness
- Ignoring TLD, registrar, hosting context
- Lack of data source transparency

Key challenges tackled:

- RBL Paradox
- Temporal Simpson's Paradox

RBLs Paradox: Many Feeds, Inconsistent Views

- Limited overlap between RBLs.
- More feeds = more disagreement.
- Single RBL = blind spots;
  multiple RBLs = contradictions.

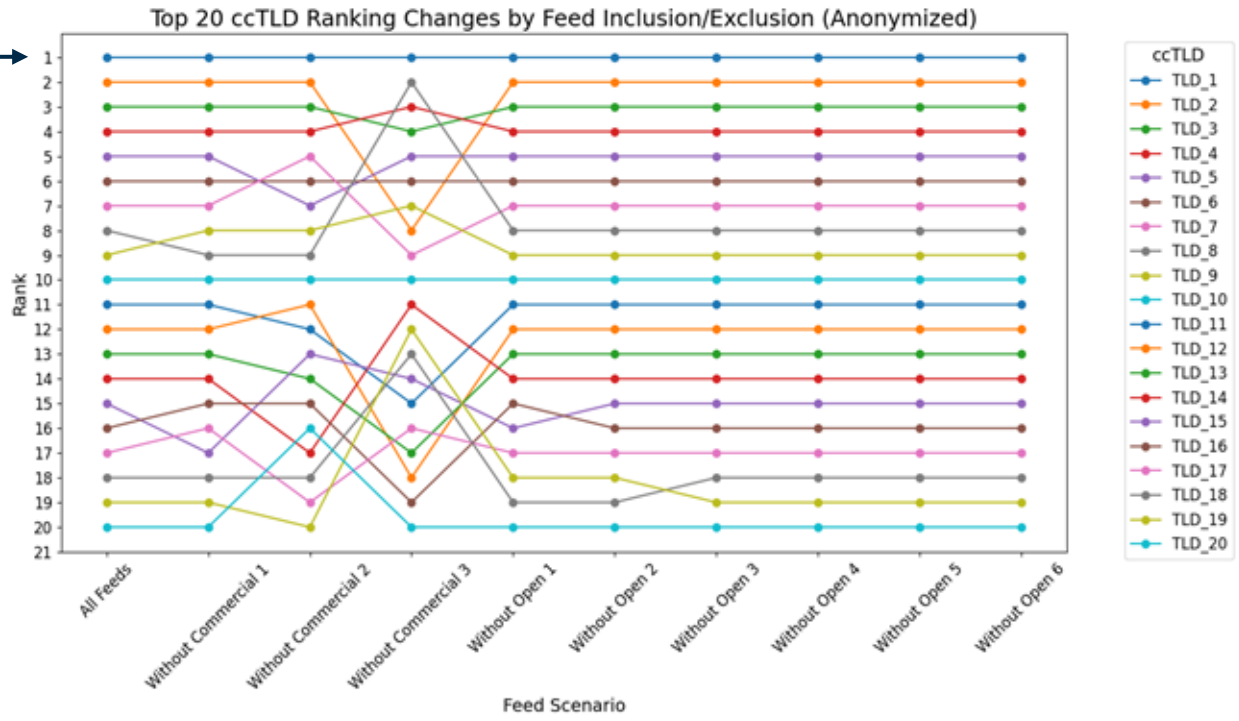
“Blindfolded people and the elephant” — each RBL feed touches part of the threat landscape, but none sees the whole.



RBL Impact: Shifting DNS Abuse Rankings

Chart demonstrates how different RBL combinations alter TLD rankings.

Highlighting the critical need for diverse, quality-controlled data.



ICANN Domain Metrica's Solution to the RBL Paradox

Diverse Data Sources:

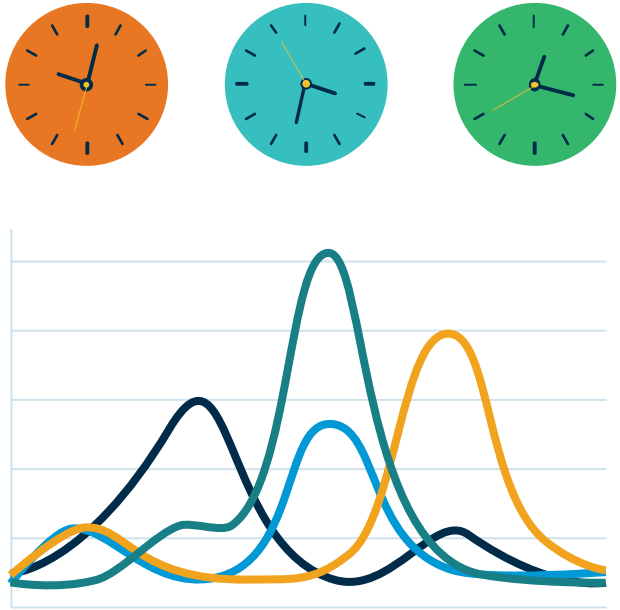
Integrates public and commercial RBLs for broad, balanced coverage.



Rigorous Quality Control:

Yearly evaluation of all input lists using OCTO037 methodology.

Temporal Simpson's Paradox: Time Distorts Metrics

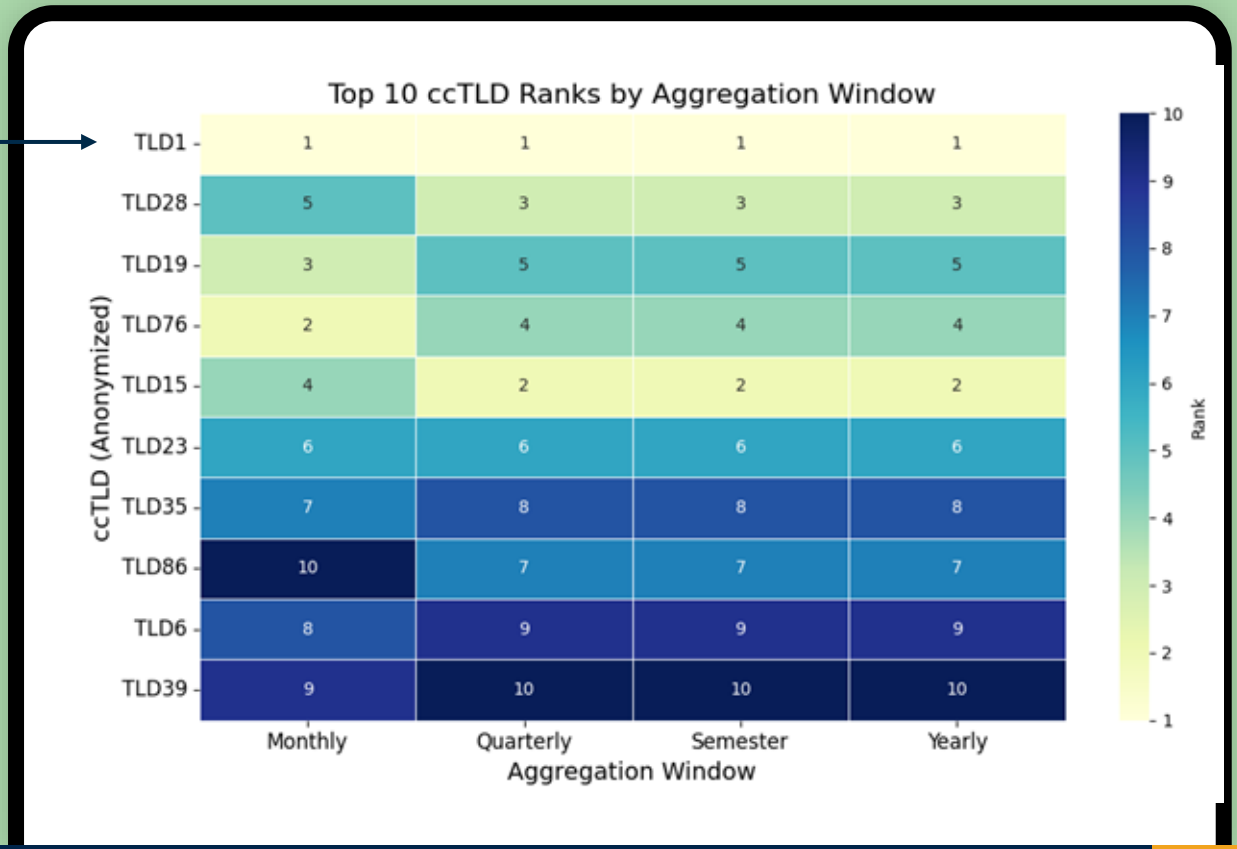


- Abuse counts vary wildly by time window (daily, weekly, monthly).
- Short windows miss long-term trends; long windows hide short-term dynamics.
- Inconsistent reporting windows make comparisons unreliable.
- Time choices can alter narratives, creating opposite stories from the same data.

Visualizing the Temporal Paradox: Rank Changes by Aggregation Window

Heatmap shows how ccTLD rankings shift with different aggregation windows.

Emphasizing the need for flexible time-series analysis.



ICANN Domain Metrica's Solution to the Temporal Paradox



Customizable Time Windows:

Define your own ranges for accurate metrics.



Lifecycle-Aware Metrics:

Accounts for domain dynamics, filters inactive domains.



Trend-Focused Analysis:

Fine-grained, time-series views reveal true trends.



Flexible Comparisons:

Ensures fair, meaningful interpretations across equivalent time spans.

ICANN Domain Metrica Data: A Foundation of Diverse Sources

Comprehensive Data Inputs:

- gTLD zone data
- Registration data
- Public and commercial RBLs
- Domain popularity rankings

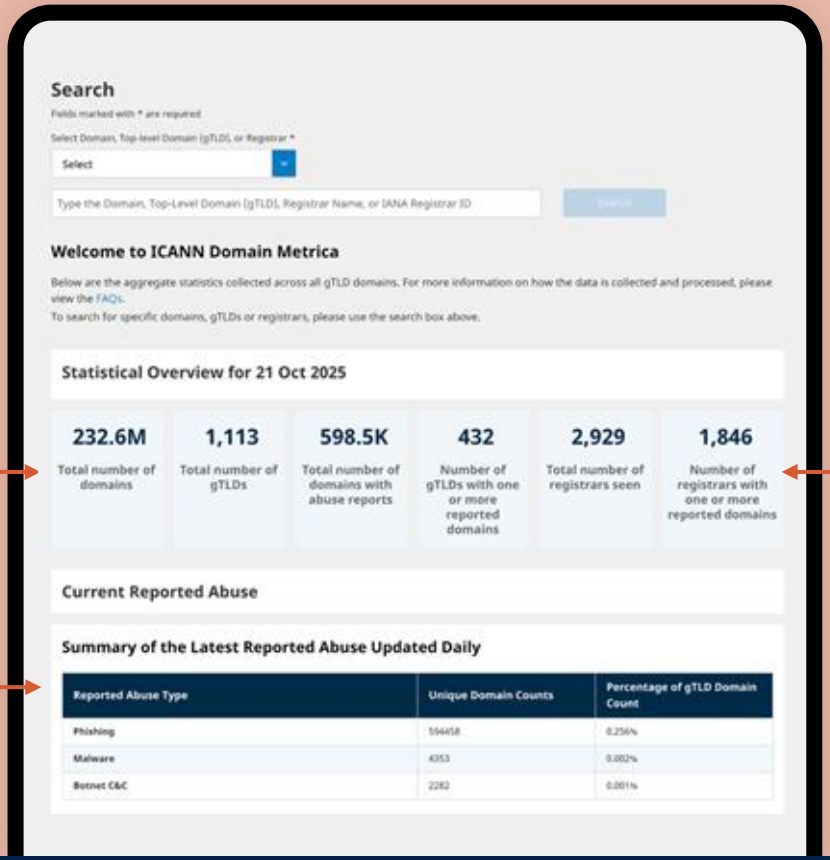
Accessible Data: Available via API and WebUI (where permitted)



Dashboard Overview: Instant DNS Abuse Statistics

Total domains, gTLDs, domains with abuse reports.

Summary of latest reported abuse by type (Phishing, Malware, Botnet C&C).



Number of gTLDs/registrars with reported domains.

12-Month Trends: Phishing & Malware in gTLDs

Visualizes median monthly reported DNS abuse.



Track historical trends for key abuse types.

ICANN Domain Metrica for ccTLDs: Enhancing Abuse Mitigation



Current Challenge: Limited ccTLD zone file access impacts data processing.

- Limits filtering non-delegated domains.
- Prevents normalized zone-based counts.



Benefits for ccTLDs: Access abuse data via MoSAPI and (when ready) UI, benchmarking insights for mitigation.



Participation Options:

- **Full Zone Files:** Maximize comparability with gTLDs.
- **Self-Report Zone Size:** Use DNS queries for existence, normalize with reported size.
- **No Data Sharing:** Still get meaningful insights via DNS queries & estimated zone size.

ICANN Domain Metrica: Continuously Evolving



Not "finished" – constantly adding features



Evolving based on community feedback and new use cases



Yearly evaluation of input lists using OCTO037 methodology



Committed to continuous improvement for a more secure Internet

Q&A

Learn More and Engage!



ICANN Domain Metrica Homepage:
icann.org/octo-ssr/metrica-en



ICANN Domain Metrica Platform:
domainmetrica.icann.org



Connect with SSR Research:
ssr-research@icann.org

ICANN Webpage and Social Media Links


icann.org


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin.com/company/icann


instagram.com/icannorg