Evaluating URL-Based Cyber Threat Intelligence Feeds:
A Proposal for a Literature-Grounded Quality Assessment Framework

Olajuwon Bello | c00326763@setu.ie | Department of Computing | SETU

A transparent, literature-grounded framework for comparing open URL-based CTI feeds over six weeks

1. Context and Gap

CTI helps organisations recognise and respond to harmful activity. But although they often know that feed quality matters, there is a lack of transparent framework for comparing open URL feeds (ENISA, 2024; Zibak, Sauerwein and Simpson, 2022)

.

Security teams use external indicators to support triage.

2. Problem, Aim and Questions

Late / stale indicators	Noise / incompleteness	Ad hoc feed selection

(Schlette et al., 2021; Chatziamanetoglou and Rantos, 2025)

Aim: To design and justify a literature-grounded framework for evaluating the quality of open, URL-based CTI feeds over a six-week period, with transparent comparison outputs.

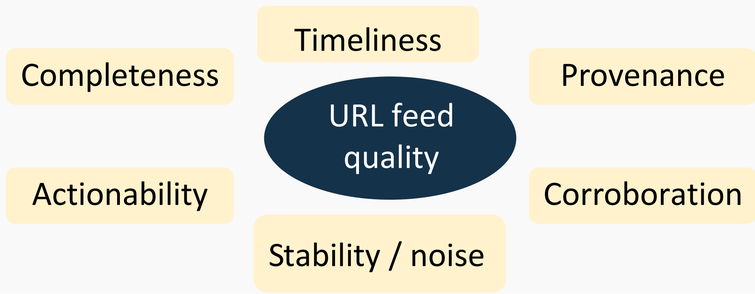
Objectives:

- Select suitable public URL-focused feeds
- Collect repeated snapshots across six weeks
- Operationalise literature-grounded quality indicators
- Build dashboard to compare feeds with indicators

3. Literature-grounded Basis

Recent studies especially by Schlette et al. (2021), Rüedlinger et al. (2024), and Chatziamanetoglou & Rantos (2025), agree that CTI quality should be measured rather than assumed, monitored over time, and compared using justified weighting choices.

Key quality dimensions



4. Methodology

Quantitative secondary-data design using repeated snapshots, harmonisation, transparent metrics and validation.

Feed sources → Repeated collection → Raw storage & logs → Cleaning & harmonisation → Metric calculation → Weighting & scoring → Validation & dashboard

Feed selection logic

- public and repeatable to collect
- URL-focused and operationally relevant
- usable timestamps / metadata
- excludes commercial or insufficiently described sources

Planned metrics

- timeliness / freshness
- corroboration proxy across feeds
- persistence and redundancy / noise
- completeness: context and provenance

Weighting and validation

- equal weights = transparent baseline
- entropy weights = sensitivity scenario
- internal consistency and time-window checks
- missing-day logs and stability review

Scope and boundaries

- secondary data only
- no visiting live malicious URLs
- comparative proxy, not ground truth
- document outages, schema changes, parser failures

5. Selected References

ENISA (2024) ENISA Threat Landscape 2024.
Schlette, Böhm, Caselli and Pernul (2021) Measuring and visualizing cyber threat intelligence quality.
Zibak, Sauerwein and Simpson (2022) Threat Intelligence Quality Dimensions for Research and Practice.
Sakellariou, Fouliras and Mavridis (2024) A Methodology for Developing & Assessing CTI Quality Metrics.
Rüedlinger et al. (2024) FeedMeter: Evaluating the Quality of Community-Driven Threat Intelligence.
Chatziamanetoglou and Rantos (2025) Weighted quality criteria for cyber threat intelligence.
Yang, Wang and Lou (2025) An automated dynamic quality assessment method for cyber threat intelligence.
Provider documentation consulted: URLhaus, ThreatFox and OpenPhish (accessed 2 April 2026).
Zibak, A., Sauerwein, C. and Simpson, A.C. (2022) 'Threat Intelligence Quality Dimensions for Research and Practice', Digital Threats: Research and Practice, 3(4), article 44. Available at: https://doi.org/10.1145/3484202.