PRESENTED TO
ICANN Community

PRESENTED BY
Saksham Jain
(NextGen@ICANN84)

DNS Abuse: Present Challenges

& Innovative Strategies for Future Solutions

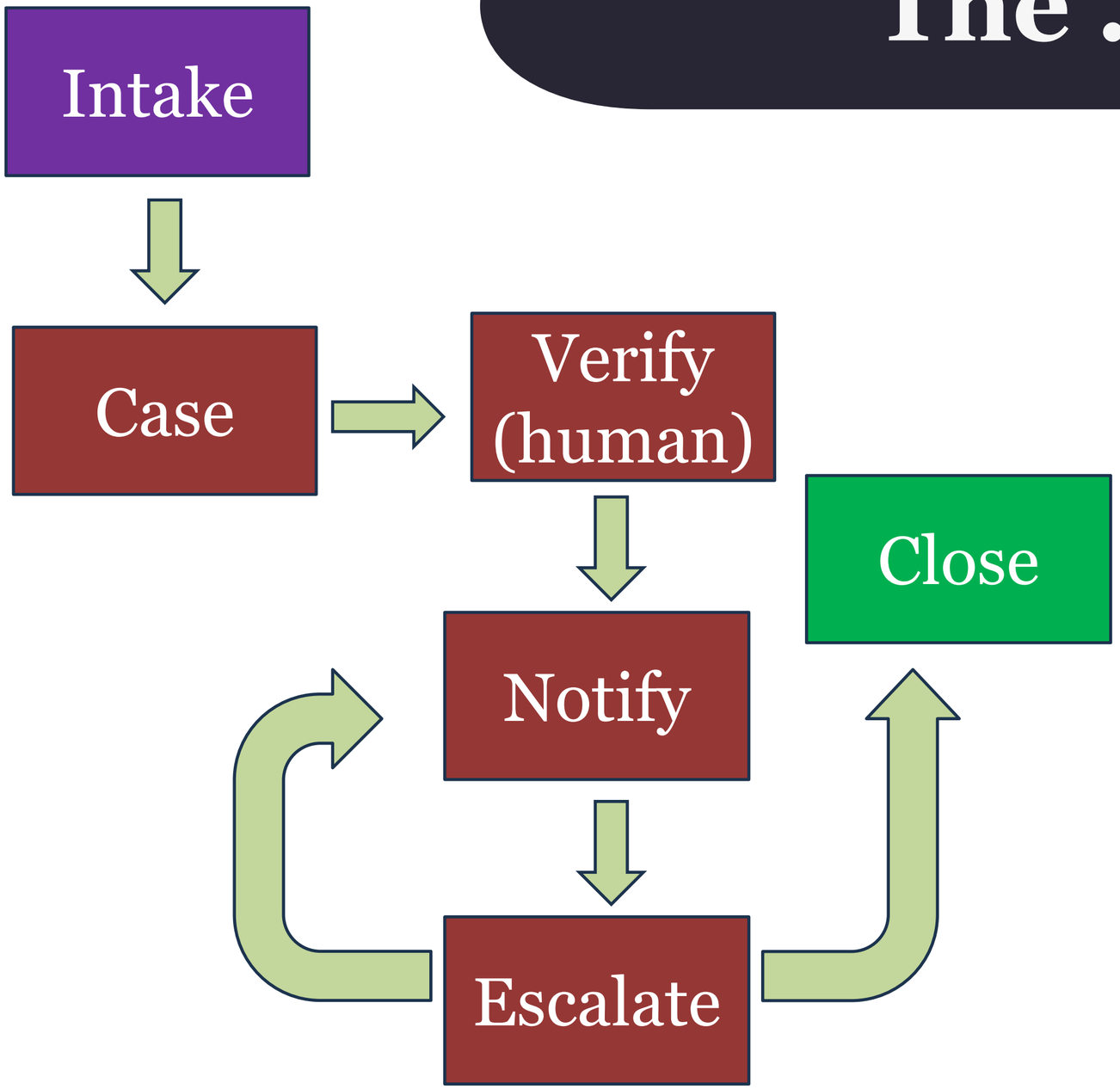
ICANN

Present challenges

- **Operational bottlenecks:** slow responses, inconsistent evidence, unclear owner of “time to fix” (registrars, resellers, registrants, etc.).
- **Evolving threats:** rapid domain turnover, AI phishing, short-lived campaigns.
- **Measurement limits:** uneven coverage, measurements guide priority but are not proof.

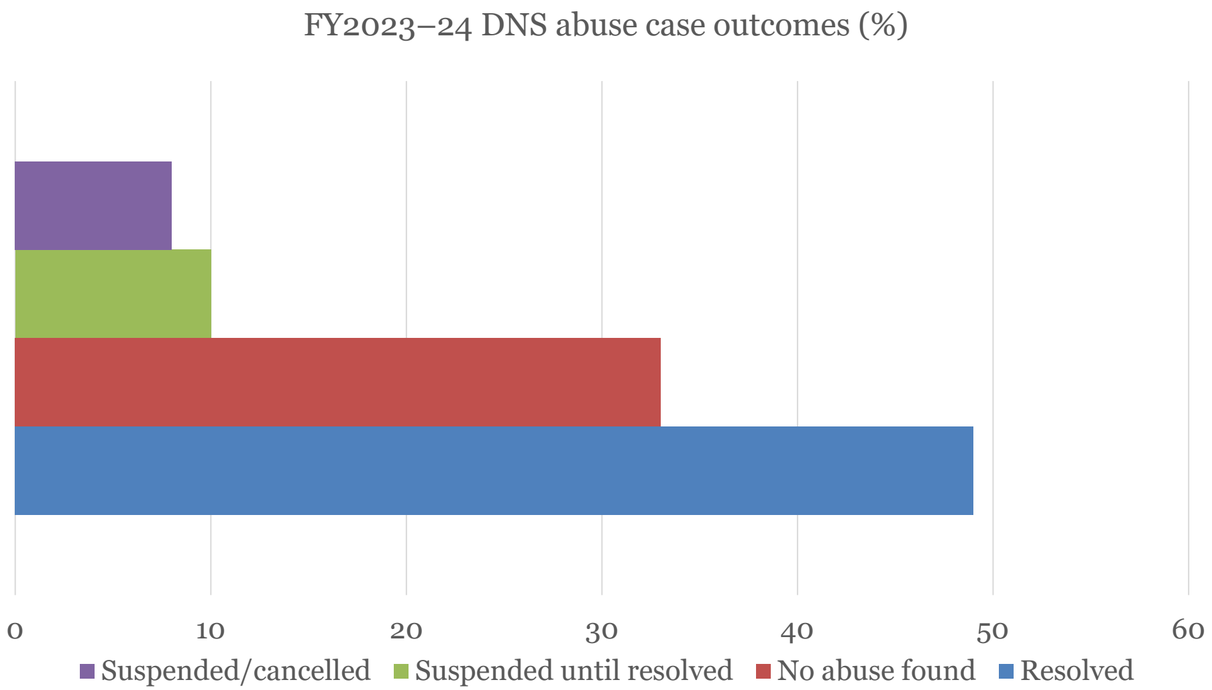
Context: ICANN contracts now expect action; NetBeacon standardises reports; measurement is directional, not determinative.

The .au method



Outcomes

Measuring effectiveness in DNS abuse mitigation efforts

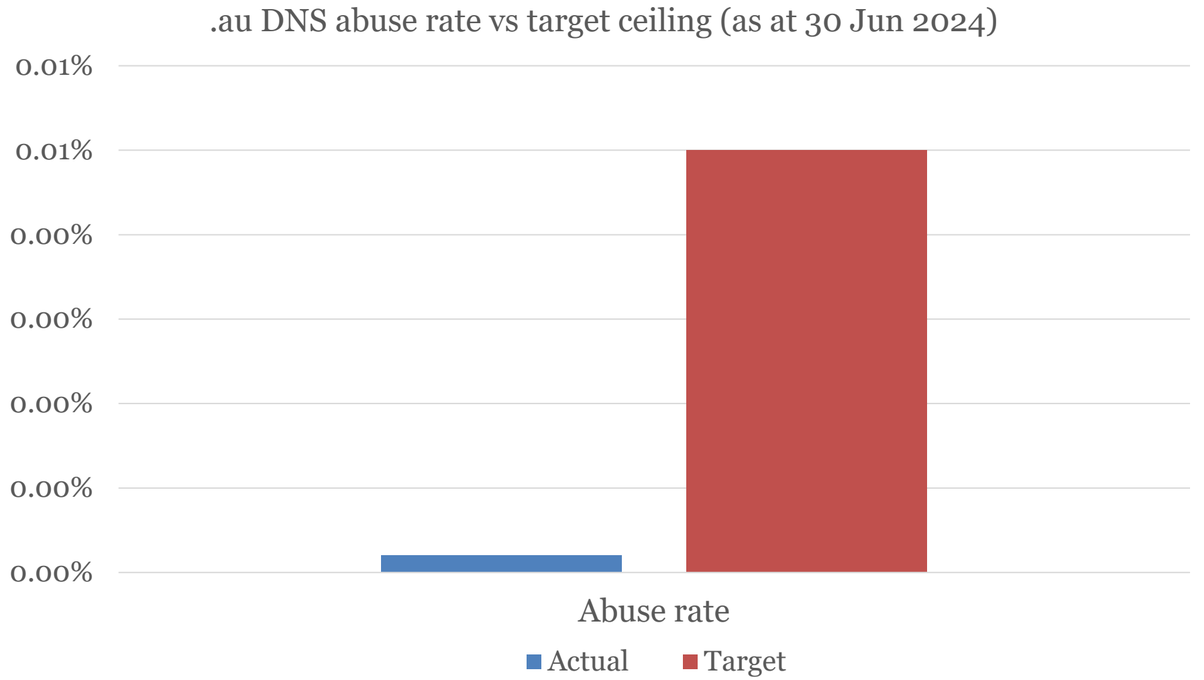


Remediation-first; suspension is rare (**18%** total)

Scope: **1,394** case reviews (FY2023–24)

Actual 0.0002%, well below the **0.005% ceiling**

Method: **confirmed active cases at year-end** (not DAAR-reported).



ICANN stakeholders

Registrars/ Resellers

Acknowledge; contact reseller/ registrant; disable/verify; own time-to-fix pre-escalation.

Registries (gTLD and ccTLD operators)

Suspension from DNS; own time-to-fix post-escalation.

Public Safety (GAC — Governmental Advisory Committee)

Standardise evidence; clear referrals.

At-Large / Internet users

NetBeacon reports with URL, timestamp, screenshots.

Law Enforcement Agencies (LEA)

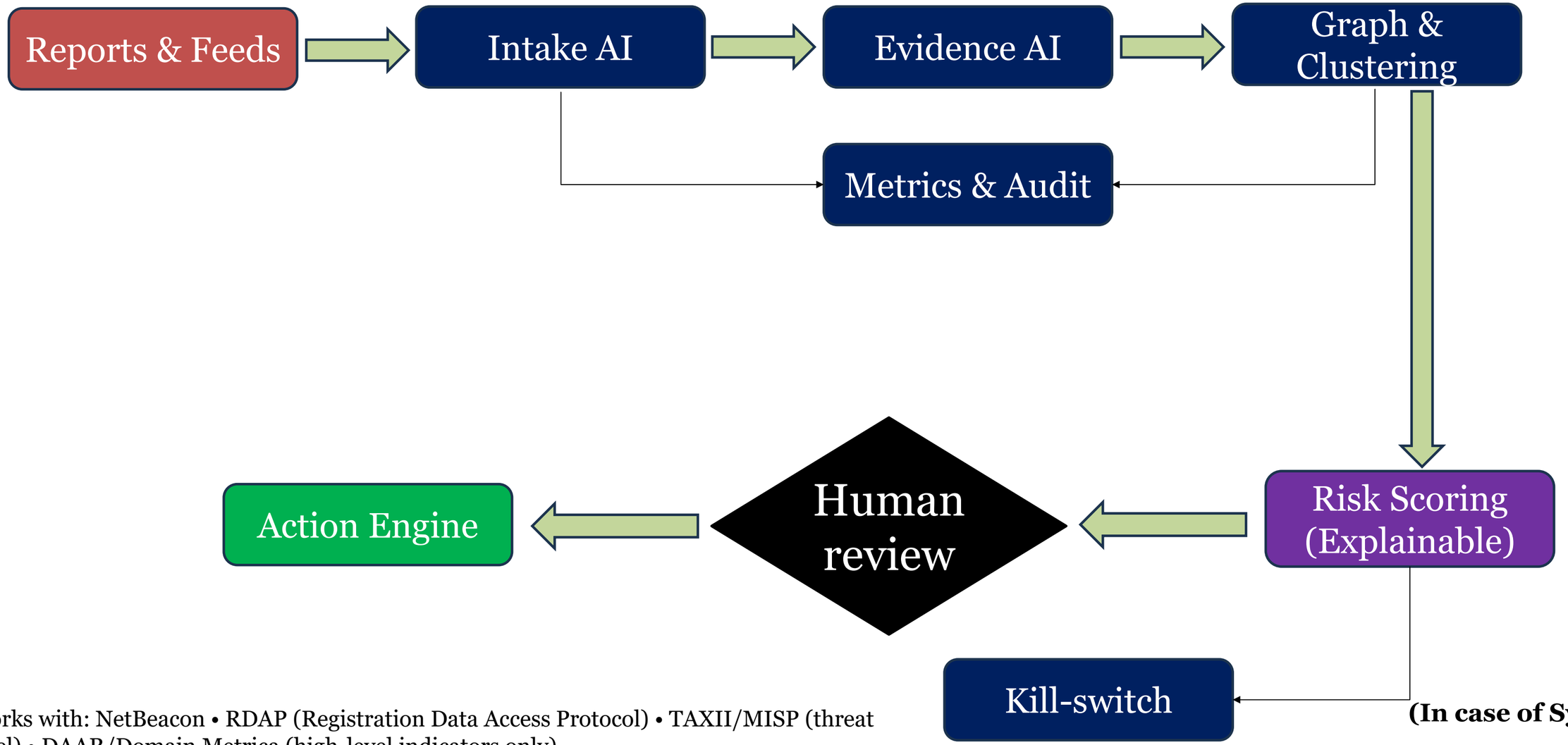
Urgent flags (if trusted notifier); preserve evidence; referral paths.

Optional: Peer exchange (ccNSO ↔ RySG)

Share playbooks and contacts; align on minimum evidence and timelines.

***Collaboration joints:** Intake = NetBeacon • Minimum evidence = URL, timestamp, screenshots, scanner reference, reporter contact • Time-to-mitigation handoff = Registrar (before escalation) → Registry (after escalation)

Proposed system



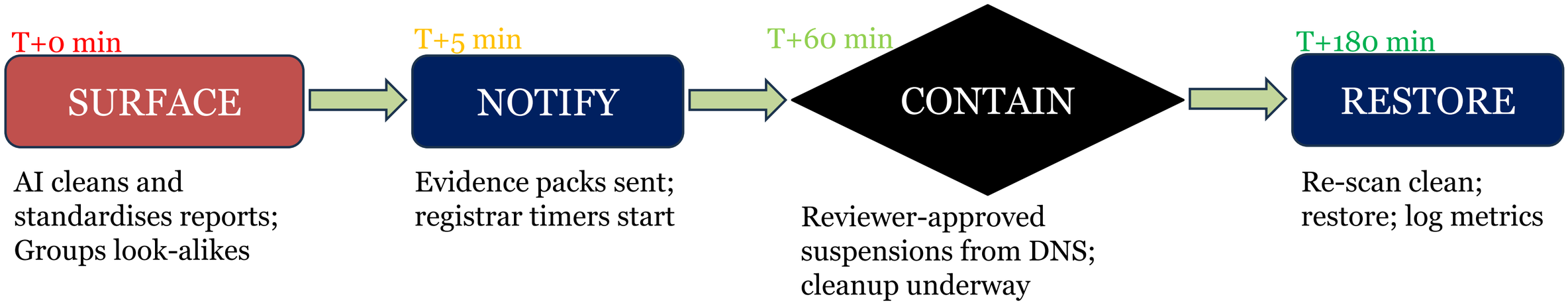
Works with: NetBeacon • RDAP (Registration Data Access Protocol) • TAXII/MISP (threat intel) • DAAR/Domain Metrica (high-level indicators only)

Proposed system

- Human verification mandatory; no model-only takedowns/ suspensions; suspensions reversible within hours.
- Kill-switch if reversals/appeals trend up.
- Privacy + audit trail for every action.
- KPIs: median/90th percentile time to fix • evidence completeness • reversals/appeals.

Hypothetical run

Key events



- **Positioning:** Extends Intake→Verify→Act→Close with AI support; **Times are illustrative**

Questions?

Get in touch:

EMAIL

sakshamjain3388@gmail.com

LinkedIn

@sakshamjainsj345