Digging in KINDNS:

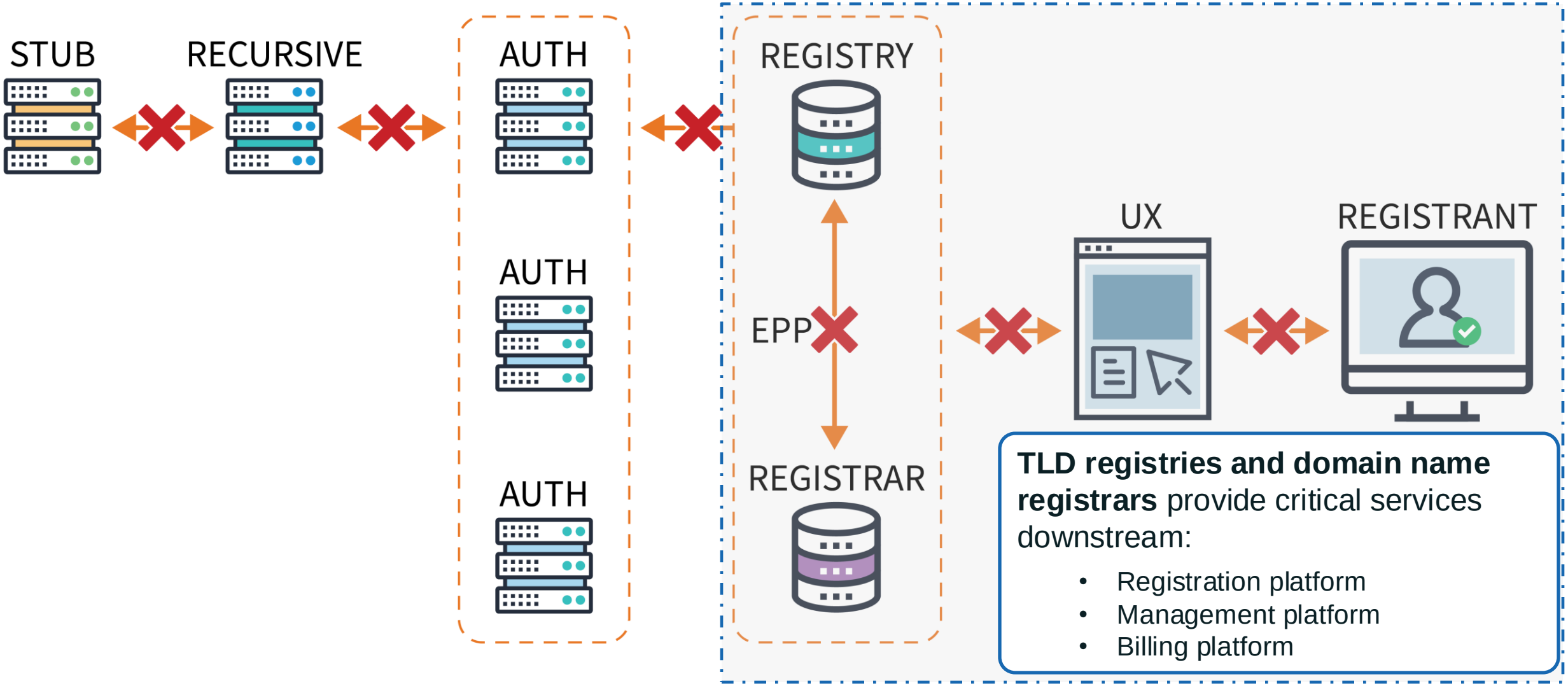
Promoting DNS Security Operational Best Practices

Pulse Internet Measurements Forum – Malaysia

24 February 2025

Champika Wijayatunga
Regional Technical Engagement Sr. Manager (APAC)

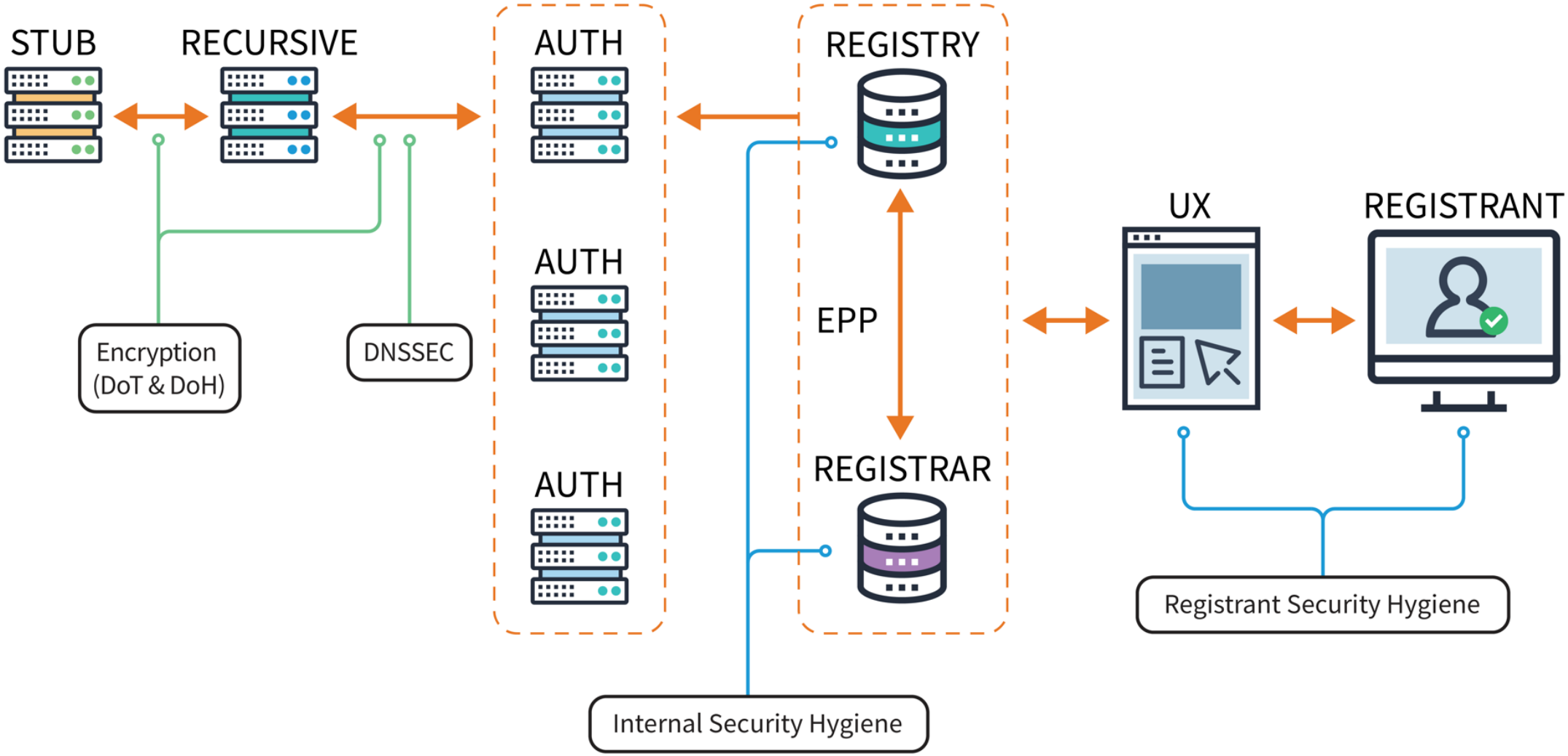
Potential Target Points of the DNS Infrastructure/Ecosystem



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

A More Secure DNS Ecosystem



KINDNS

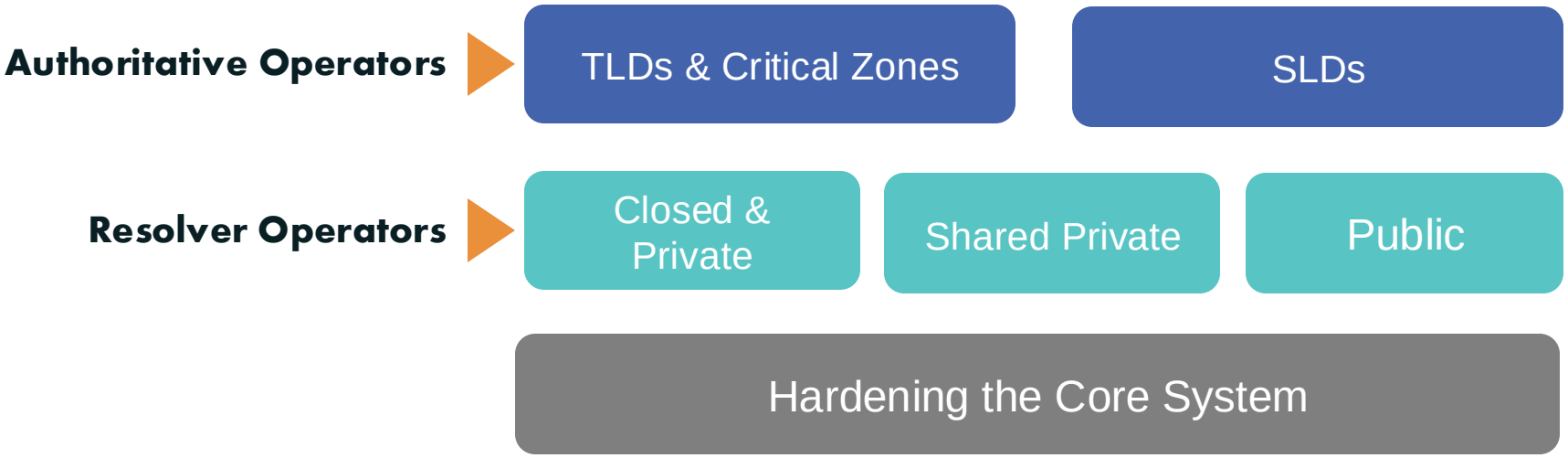
Knowledge-sharing and
Instantiating
Norms for
DNS (Domain Name System) and
Naming
Security

….. is pronounced ”kindness.”

KINDNS – Promoting DNS Operational Best Practices

An initiative to produce something simple that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices the industry identifies for better security and more effective DNS operations.

Targeted Operators



By joining the KINDNS initiative, DNS Operators are voluntarily committing to adhere to the identified practices and act as "goodwill ambassadors" within the community.

Self-Assessment & Reports

- Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices
  - Self-Assessments will be anonymous, and a report can be directly downloaded from the web site
- Operators can enroll to participate in one or many categories covered by KINDNS
  - Participation in KINDNS mean voluntarily committing to implement and adhere to agreed norms and practices
  - Participants becomes goodwill ambassadors and promote practices

Self-Assessment & Reports

Response	% of responses
To know where I stand with KINDNS practices	72.57%
To join KINDNS	30.98%
To use the result to convince my organization to do better securing our DNS operations	41.86%
Other	9.73%

Self-Assessment & Reports

- As Authoritative Nameserver manager for one or more TLDs or Critical Zones, I implement and adhere to the following practices:

Response	% of responses
Practice 1: My authoritative zones are DNSSEC signed and I follow best practices for key management	68.86%
Practice 2: Access to zone transfer between authoritative servers is restricted to secondary servers only (use of ACLs and/or TSIG to restrict zone transfers)	68.86%
Practice 3: I have a process in place to check the integrity of my zone file/data	51.69%
Practice 4: My authoritative nameservers are running on separate servers from my recursive resolvers.	68.64%
Practice 5: I am using at least two distinct nameservers for each critical zone under my control	63.77%
Practice 6: My network infrastructure adheres to basic network security best practices (BCP38/MANRS)	50.85%
Practice 7: The infrastructure that serves my DNS service is actively monitored	58.26%
Practice 8: My authoritative servers run on an infrastructure that takes operational diversity into account	49.36%

Self-Assessment & Reports

- As Operator of Authoritative Nameserver(s) for one or more Second Level Domains (SLDs), I implement and adhere to the following practices:

Response	% of responses
Practice 1: My authoritative zone(s) is/are DNSSEC signed and I follow key management best practices.	54.58%
Practice 2: Access to zone transfer between authoritative servers is restricted to secondary servers only	76.95%
Practice 3: I have a process in place to check the integrity of my zone files	49.49%
Practice 4: My authoritative nameservers are running on separate servers from my recursive resolvers.	73.39%
Practice 5: I am using at least two distinct nameservers for each zone under my control with topological and geographical diversity considerations	66.78%
Practice 6: The infrastructure that serves my DNS service is actively monitored	75.93%

Self-Assessment & Reports

KINDNS

- As a Shared Private Recursive Resolver Operator, I implement and adhere to the following practices:

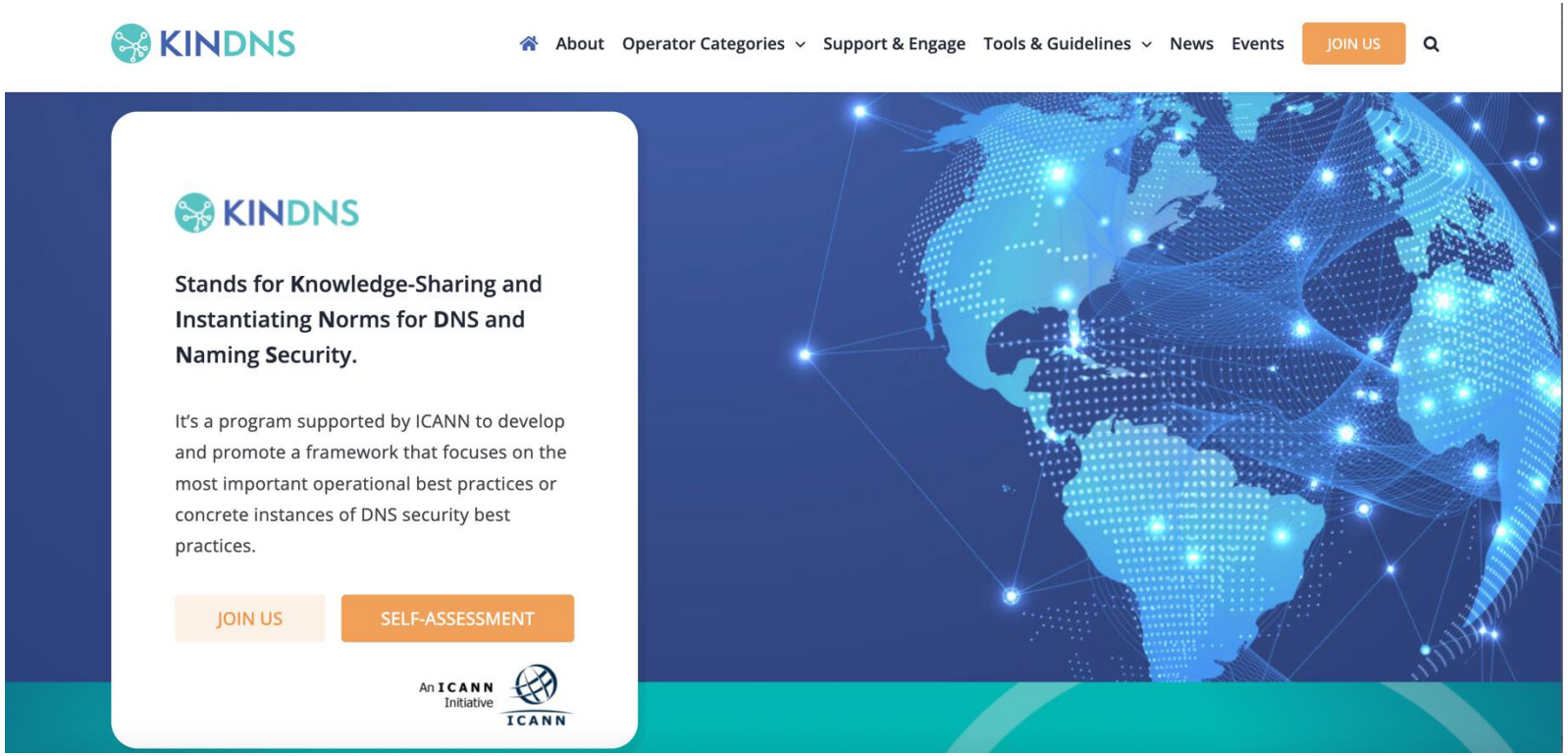
Response	% of responses
Practice 1: I have DNSSEC validation turned on for my resolvers	65.70%
Practice 2: I use ACLs to restrict who may send recursive queries to my resolvers	79.71%
Practice 3: I have QNAME minimization turned on for my resolvers	44.44%
Practice 4: My resolvers don't run on the same server as any authoritative DNS services	58.94%
Practice 5: My recursion services are resilient; using at least two distinct servers that take diversity into consideration	57.97%
Practice 6: The infrastructure that serves my DNS service is actively monitored	64.73%

Self-Assessment & Reports

- Do you have proper credential management practices and processes implemented?

How to Stay Informed and Contribute

- https://www.kindns.org



- **The KINDNS discussion mailing list:** kindns-discuss@icann.org

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann