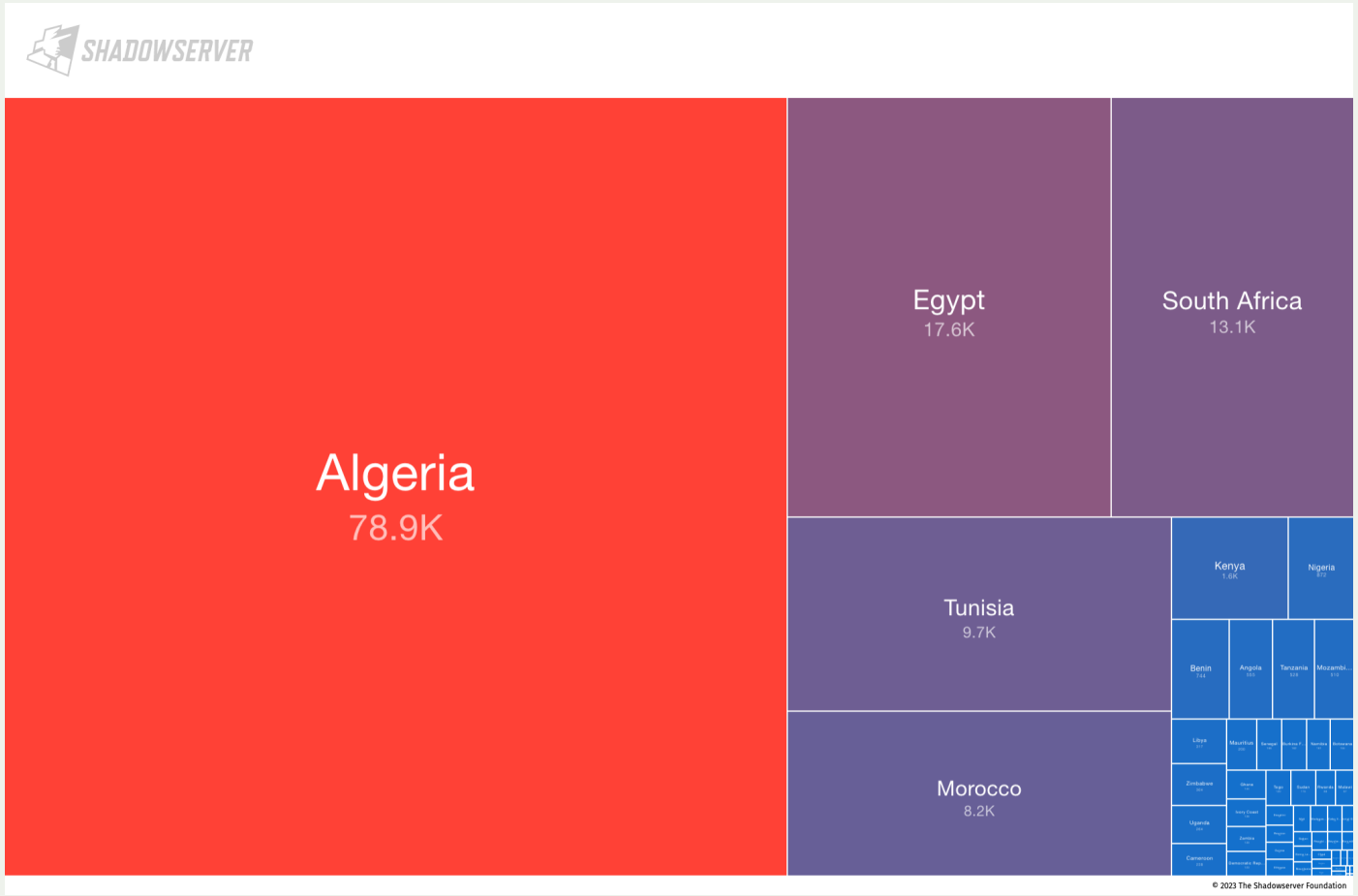
23 March 2023

ZANOG-23

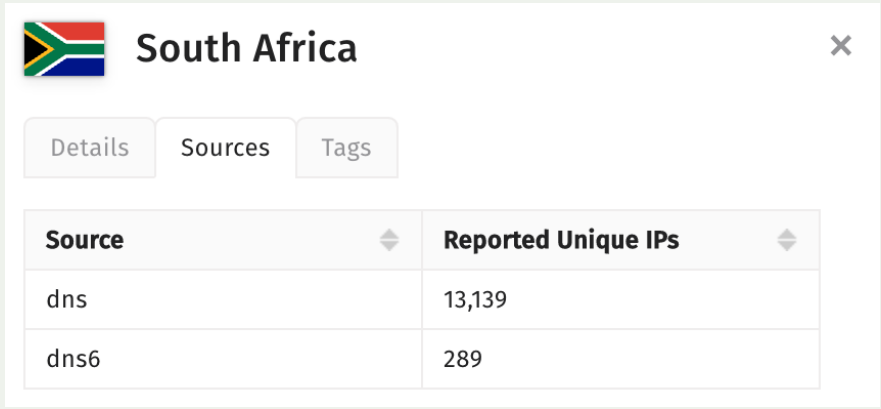
Measuring DNS Hygiene

Amreesh Phokeer
phokeer@isoc.org

How bad is your hygiene?

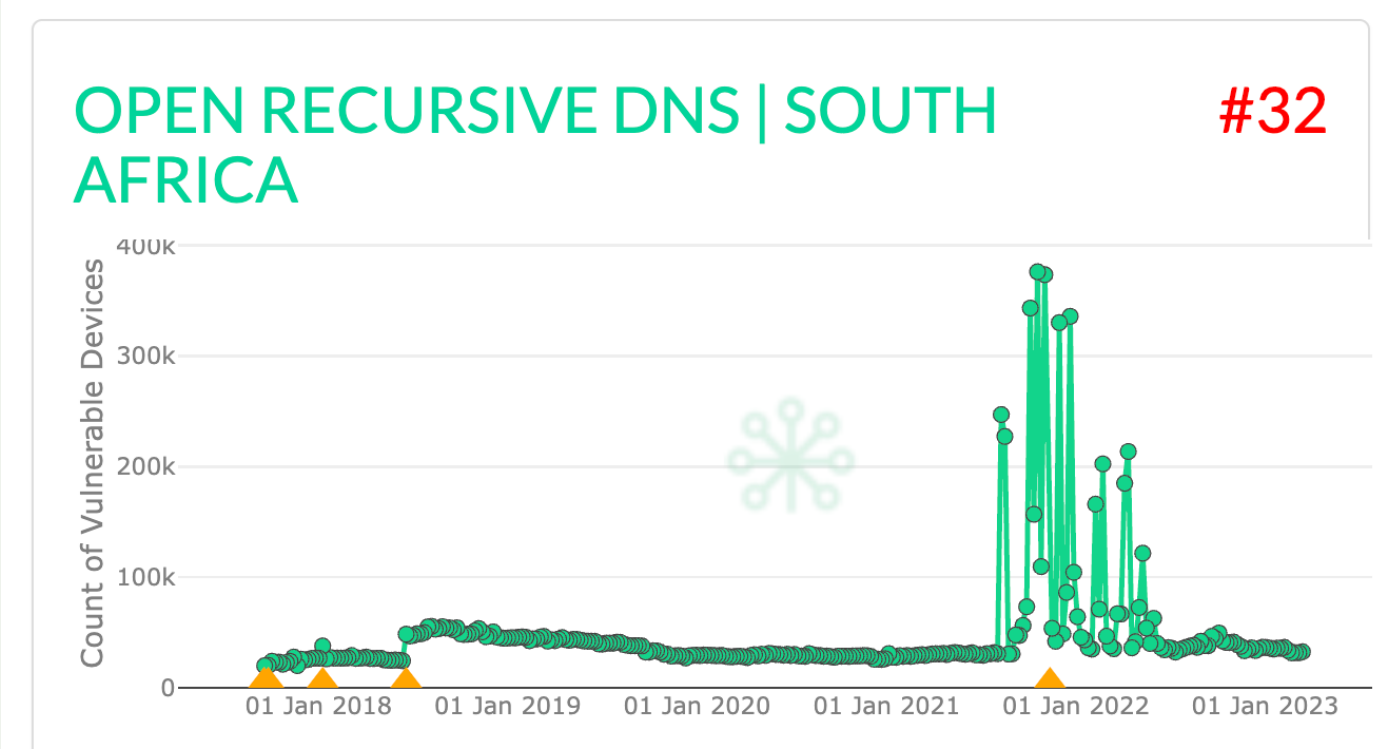


Open Resolvers

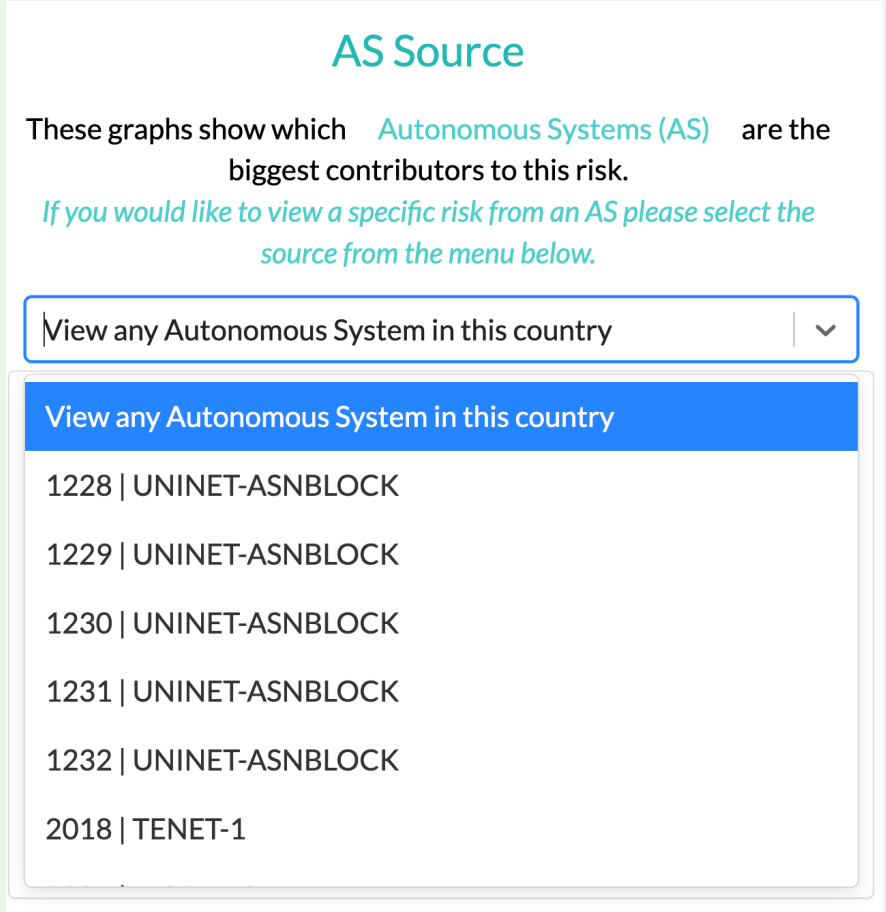


https://dashboard.shadowserver.org/statistics/combined/tree/?day=2023-03-21&source=dns&tag=openresolver&geo=Africa&data_set=count&scale=log

How bad is your hygiene?



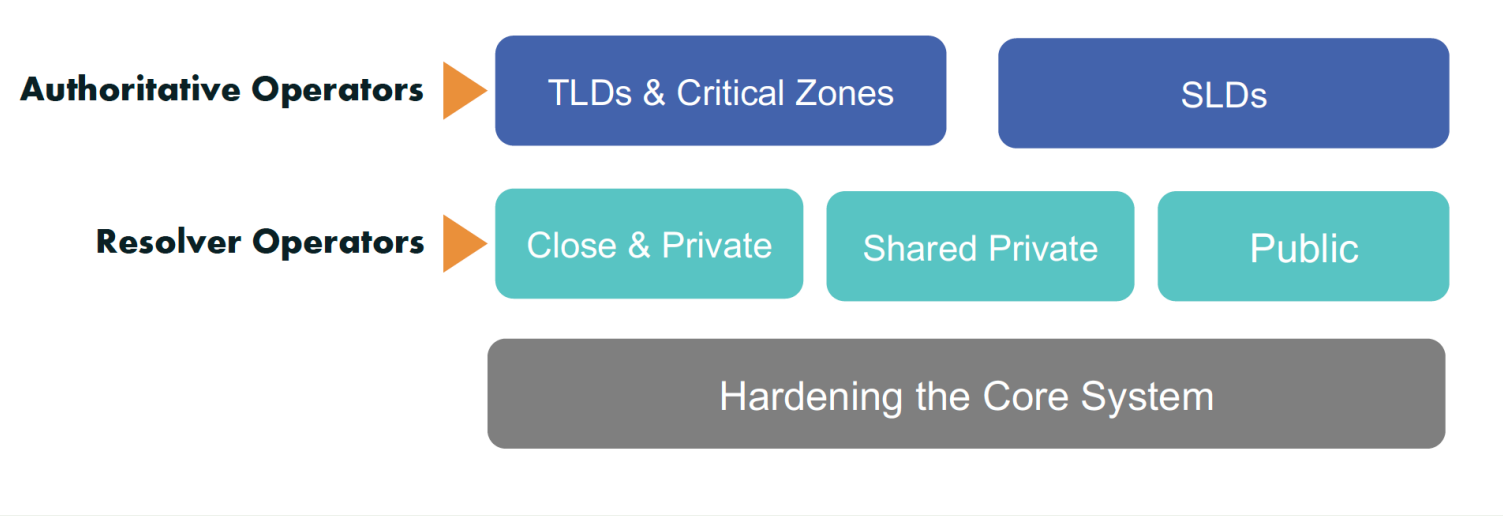
https://stats.cybergreen.net/country/south-africa/



ICANN KINDNS – KINDNS.ORG

Knowledge-Sharing and Instantiating Norms for DNS and Naming Security

- An initiative to produce something simple to refer to 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 that the industry identifies for better security and more effective DNS operations.
- Each category has 6-8 practices that ICANN will encourages operators to implement.
- By joining KINDNS, DNS operators are voluntarily committing to adhere to these identified practices and act as "goodwill ambassadors" within the community.



KINDNS SELF-ASSESSMENT

Authoritative DNS Operators of Critical Zones

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Authoritative DNS Operators of SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Closed & Private Resolver Operators

1. DNSSEC validation **MUST** be enabled
2. Access control list (ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. Authoritative servers for a given zone **MUST** run from a diversified Infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Shared Private Resolver Operators

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. **For pr**ivacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Closed/Open Public Resolver Operators

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. **For pr**ivacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Hardening the core

1. ACLs **MUST** be implemented to control network traffic to your DNS servers
2. BCP38/MANRS egress filtering **MUST** be implemented
3. The configuration of each DNS server **MUST** be locked down
4. User permissions and application access to system resources **MUST** be limited
5. System and service configuration files **MUST** be versioned
6. Access to management services **MUST** be restricted
7. Access to the system console **MUST** be secured using cryptographic keys and/or two factor authentication mechanism.
8. Credentials Management for customer access **MUST** adhere to best practices

What can we actually measure?

Measurable Practices

- Focus only on public-facing DNS infrastructure: open resolvers and authoritative nameservers
- Identify practices that are not measurable and suggest practices based on previous scientific studies
- For each practice, the main goal, data required for independent validation, relevant measurement tools are identified

What can be measured?

- DNSSEC Adoption (Active Scans, e.g., OpenINTEL, Rapid7)
- Geographically, Topologically, NS Diversity (Active Scans)
- QNAME minimization (Passive and Active Scans)
- MANRS/BCP38 compliancy (Spoofer)
- Authoritative and Recursive DNS software not on the same server - Focus on Open Resolvers
- ACLs and non-DNS service exposure (Port Scans) - Focus on well-known ports
- DoH/DoT adoption in the wild
- Software Diversity (Fingerprinting) >>>> Challenging

Some statistics (Sommese et al. ACM IMC'22)

Over 638K authoritative nameservers IPs :

- 52% have web port (80) open
- ~40% have mail ports open (25, 995, etc.).
- 31% have SSH port open
- Other popular ports open are: (s)FTP, Windows Share, SUN RPC
- 1.5% of authoritative are recursion enabled!

Some statistics (Sommese et al. ACM IMC'22)

Over 1613K recursive resolvers IPs:

- 8% have web port (80) open
- 6% have SSH port open
- 5% have Telnet port open!!
- Also see mail and other services
- Only 85 DoH properly configured recursive resolvers and 78 DoT

Non-measurable practices

- Monitoring
- Internal ACL
- SSH Authentication requirements
- Server hardening, integrity and versioning

Missing measurable practices

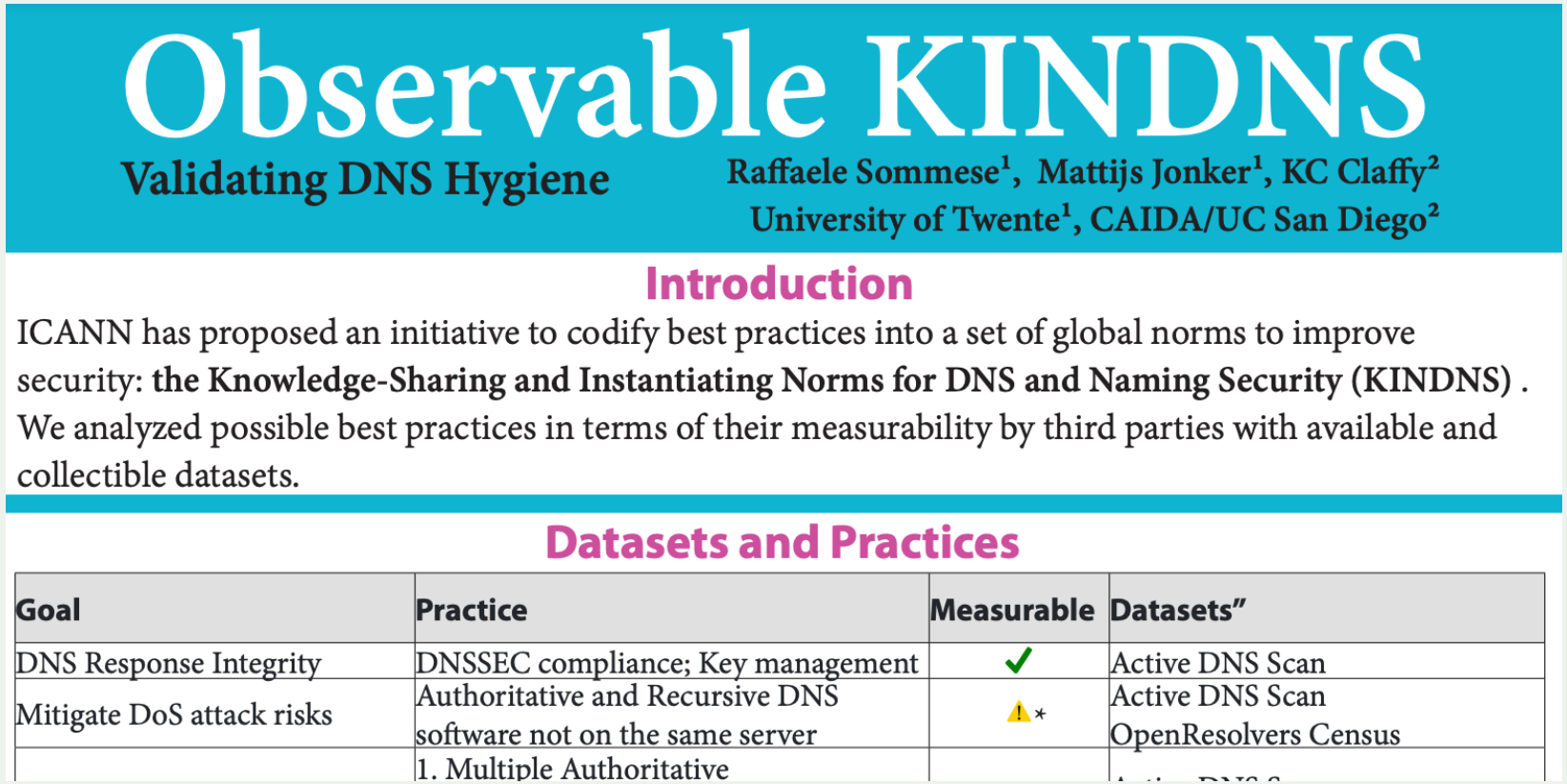
- **Anycast deployments for critical zones**: Several studies have demonstrated the value of anycast deployments of critical DNS infrastructure to increase the DNS resilience against DDoS attacks. Anycast is a de-facto standard with peaks of 97% of TLDs.
- **DNS Provider diversity**: The Dyn 2016 incident and previous studies illustrated the importance of relying on different providers (ASN) for increase DNS resilience.
- **Caching Best Practice**: Long TTL values for DNS infrastructure records increase resilience against DDoS attacks.
- **Prevent inconsistent and lame delegations** to mitigate risk of domain hijacking, especially for critical zones. Researchers have found this vulnerability has affected multiple TLDs and prominent SLDs.

References

How to measure KINDNS?

Raffaele Sommese[1], Georgia Christou[1], Mattijs Jonker[1], KC Claffy[2]

ACM IMC'22 Poster



Observable KINDNS

Validating DNS Hygiene

Raffaele Sommese[1], Mattijs Jonker[1], KC Claffy[2]
University of Twente[1], CAIDA/UC San Diego[2]

Introduction

ICANN has proposed an initiative to codify best practices into a set of global norms to improve security: **the Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS)** . We analyzed possible best practices in terms of their measurability by third parties with available and collectible datasets.

Datasets and Practices

Goal	Practice	Measurable	Datasets"
DNS Response Integrity	DNSSEC compliance; Key management	✓	Active DNS Scan
Mitigate DoS attack risks	Authoritative and Recursive DNS software not on the same server	⚠*	Active DNS Scan OpenResolvers Census
	1. Multiple Authoritative		

Thank you.

phokeer@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120