Jeff Bedser

CEO - iThreat Cyber Group

Officer - Public Interest (.ORG) BoD

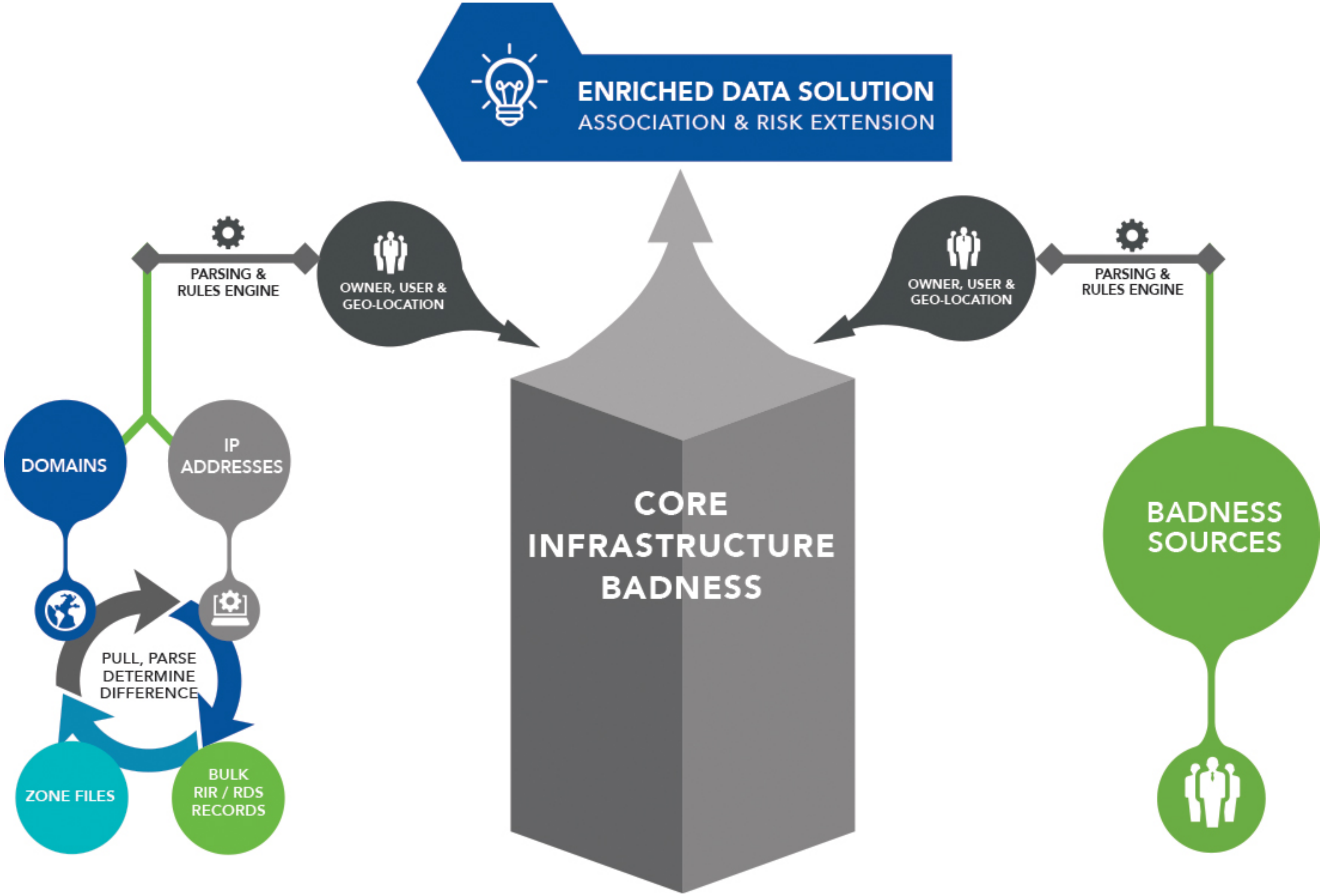
Member - Security & Stability Advisory Committee - ICANN

Last Twenty Years or so….

- iThreat has conducted investigations for cyber related activities since 1997
- PaaS Systems for cyber investigations since 2012
  - www.cybertoolbelt.com
  - Used by multiple law enforcement agencies
- PaaS System for Prescriptive and Predictive Intelligence Gathering and Analysis
  - www.ithreatfusion.center
  - Used by major international corporations
- Enriched Data Solutions

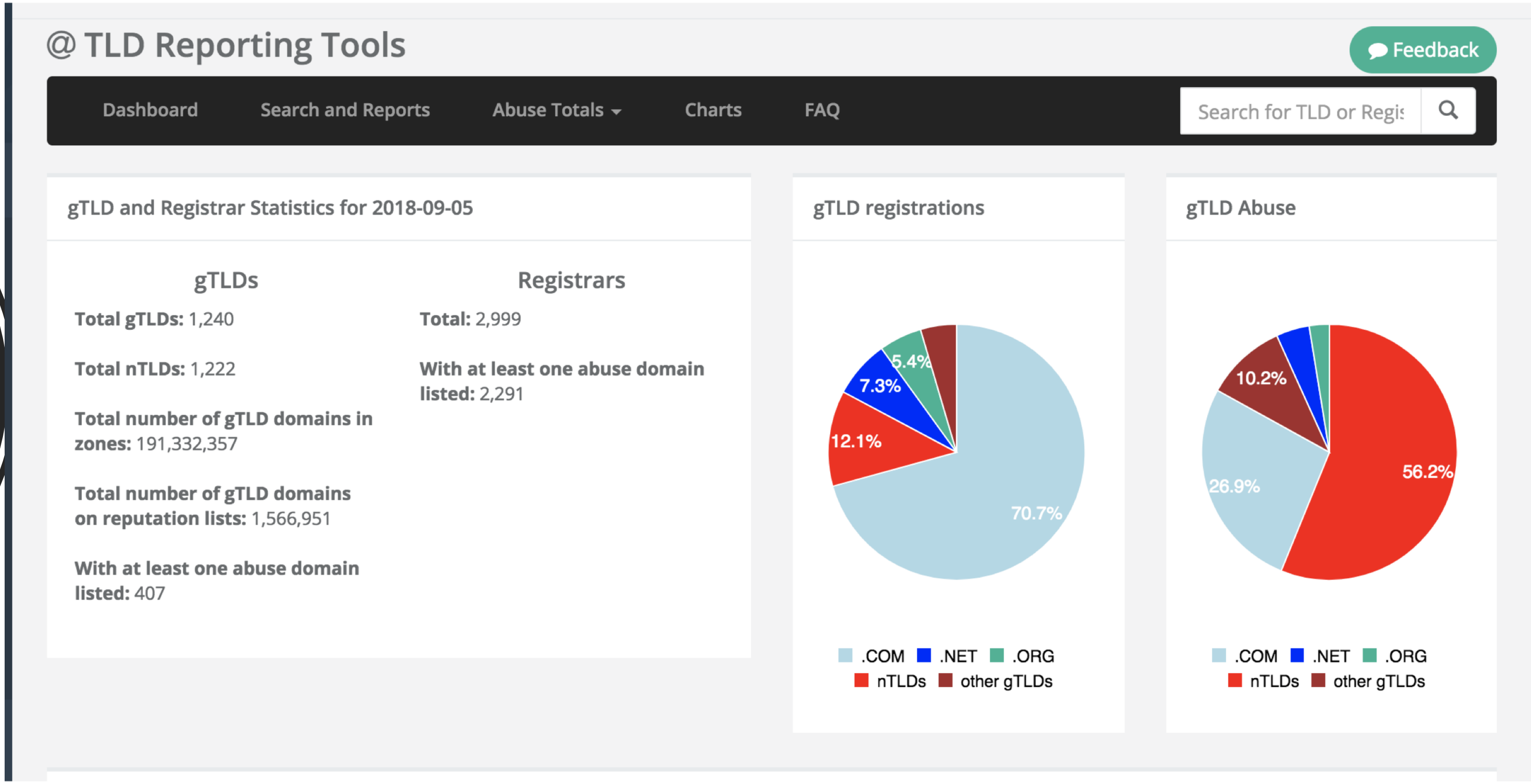
Investigation, Analysis and Awareness Targets

- Bad Actors
- Malicious Activity/Intent
- Enriched & Structured RDS data
- Reported Badness Indicators
- Infrastructure directly tied to Badness
- Infrastructure tied to badness by ownership or use
- Ties to untrusted nation-states
- Ties to Dark Infrastructure
- Hacker Forums & Haunts
- Hate Groups
- Organized crime
- Financial Crime
- Ecommerce
- Fraud
- Intellectual Property Theft
- Phishing
- Spam
- Malware
- Botnet/Botnet C&C
- IP addresses
- Domains
- Subdomains


ENRICHED DATA SOLUTION
ASSOCIATION & RISK EXTENSION
PARSING & RULES ENGINE
OWNER, USER & GEO-LOCATION
OWNER, USER & GEO-LOCATION
PARSING & RULES ENGINE
DOMAINS
IP ADDRESSES
PULL, PARSE DETERMINE DIFFERENCE
ZONE FILES
BULK RIR / RDS RECORDS
CORE INFRASTRUCTURE BADNESS
BADNESS SOURCES

…We Measure…

gTLD Domain Abuse Measurement



@ TLD Reporting Tools

Feedback

Dashboard | Search and Reports | Abuse Totals ▾ | Charts | FAQ | Search for TLD or Regis

gTLD and Registrar Statistics for 2018-09-05

gTLDs

Total gTLDs: 1,240

Total nTLDs: 1,222

Total number of gTLD domains in zones: 191,332,357

Total number of gTLD domains on reputation lists: 1,566,951

With at least one abuse domain listed: 407

Registrars

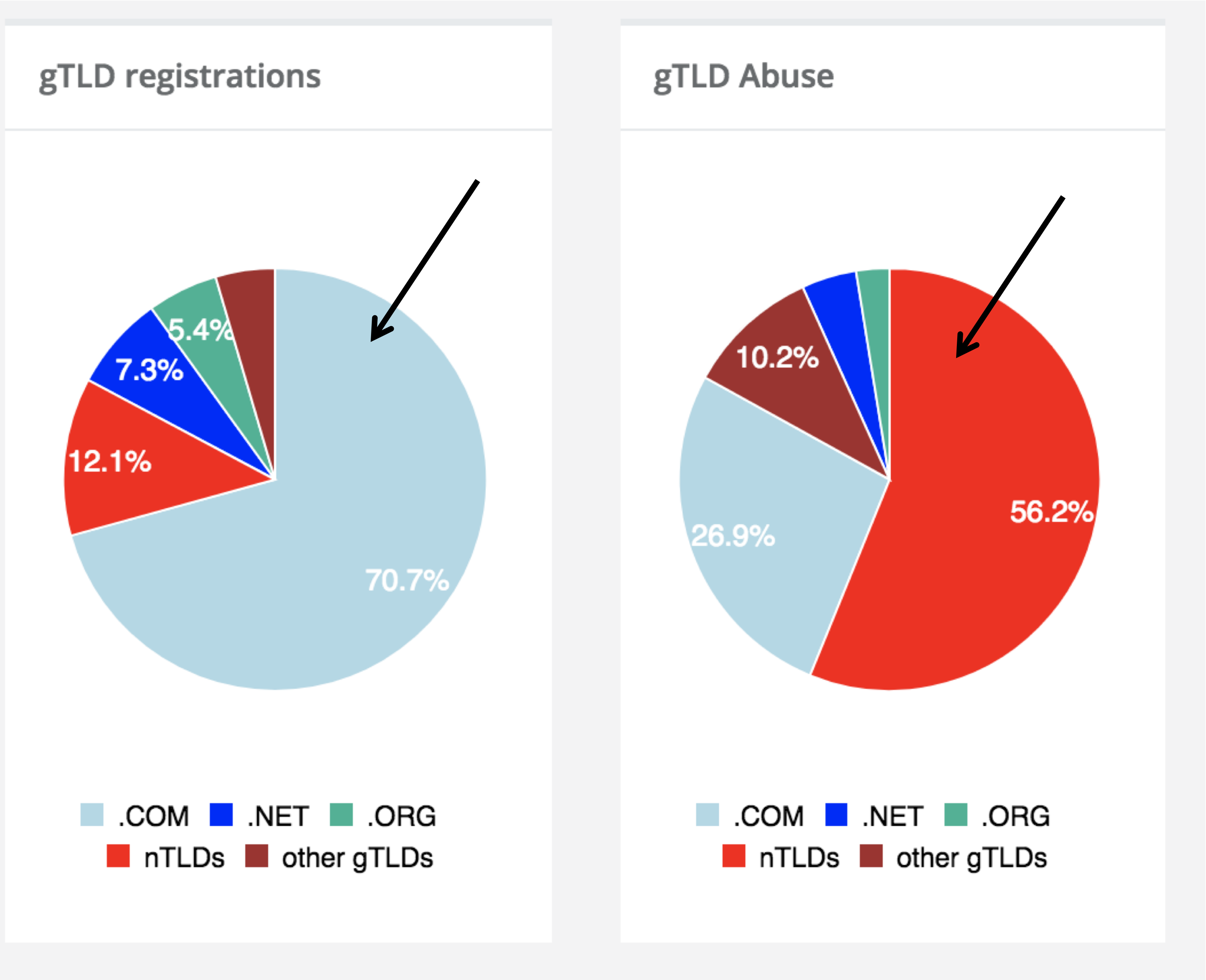
Total: 2,999

With at least one abuse domain listed: 2,291

gTLD registrations

gTLD Abuse

Does this seem right?



gTLD registrations

gTLD Abuse

*As of Sept 6, 2018

We work (volunteer) with…

- ICANN – Security & Stability Advisory Committee
- MAAWG – Messaging Anti-Abuse Working Group
- APWG – Anti-Phishing Working Group
- Coordination Center For TLD RU
- IETF – Internet Engineering Taskforce

We work to make an impact…

- Change the understanding of DNS based abuse and crime
- Change the policies of DNS operators regarding abuse
- Change the behaviors and response to abuse
- Educate global law enforcement
- Educate consumers/victims
- Provide data to better secure systems from DNS based abuse