Elegant CHAOS

Project Leads: [redacted]

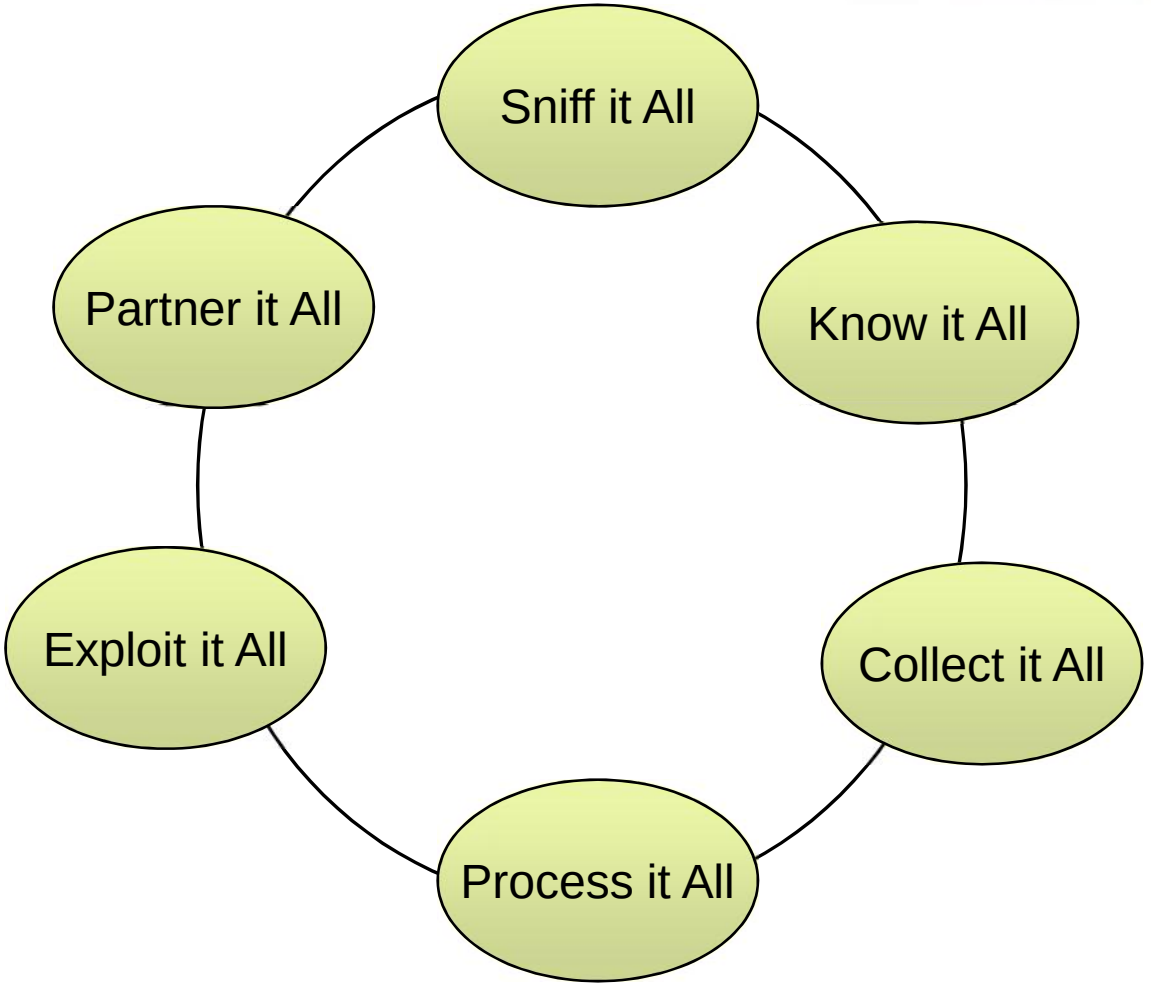
Code Support: [redacted]

For more up-to-date information please visit this URL:

[redacted]Elegant_Chaos

For recent developments please contact the authors.

Field Site Responsibilities



For Better Or Worse…

Collection access is increasing,

- software modems (ASPHALT/A-PLUS)
- new hardware/software solutions (STORMFORCE modems and DARKQUEST auto-survey)
- new physical capacity (TORUS antennae)

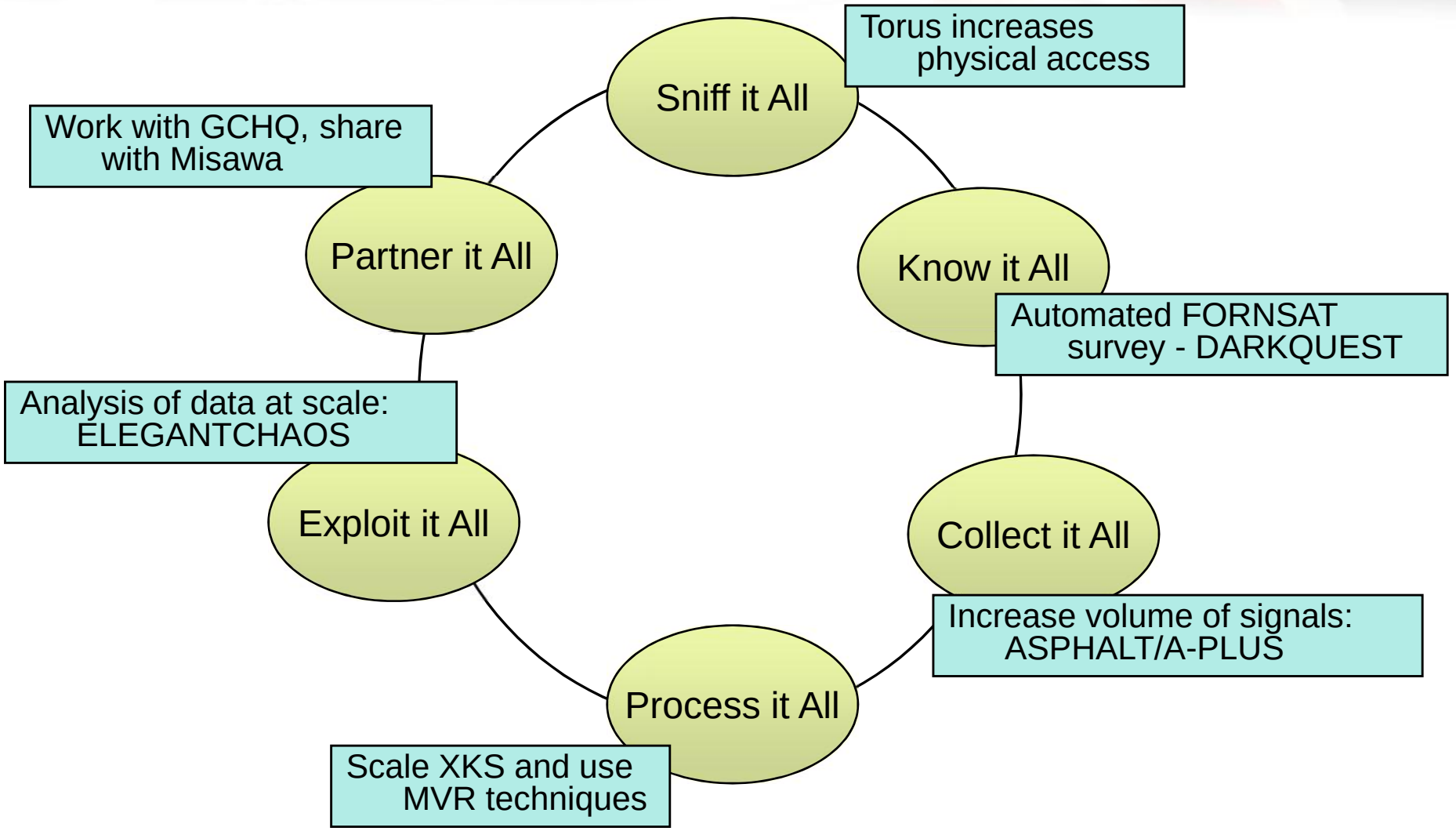
Processing capabilities are increasing,

- JCE, TINT, XKS Deep Dive

But size of analytic workforce is not!

- more resources = more resource management

New Collection Posture



ELEGANTCHAOS Goals

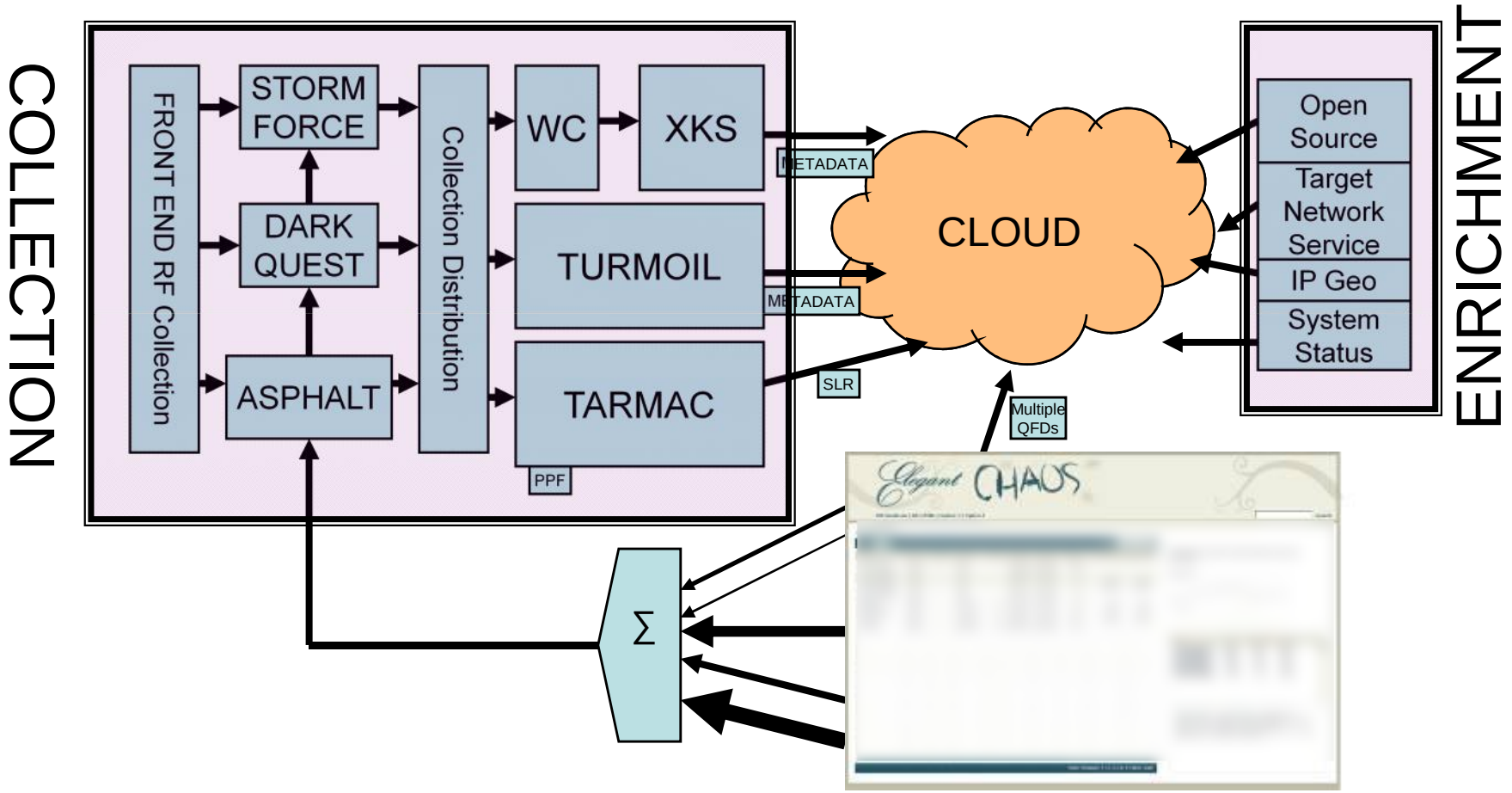
- Goal: perform basic, time-sensitive analysis on all of MHS collection
- Goal: create a prioritized list of signals (case notations) in our viewing arc
- Goal: use this list to *automatically drive collection* as collection capabilities increase
- Offshoot goal: create a product that analysts and collection managers can use to see into the system

ELEGANTCHAOS + Cloud

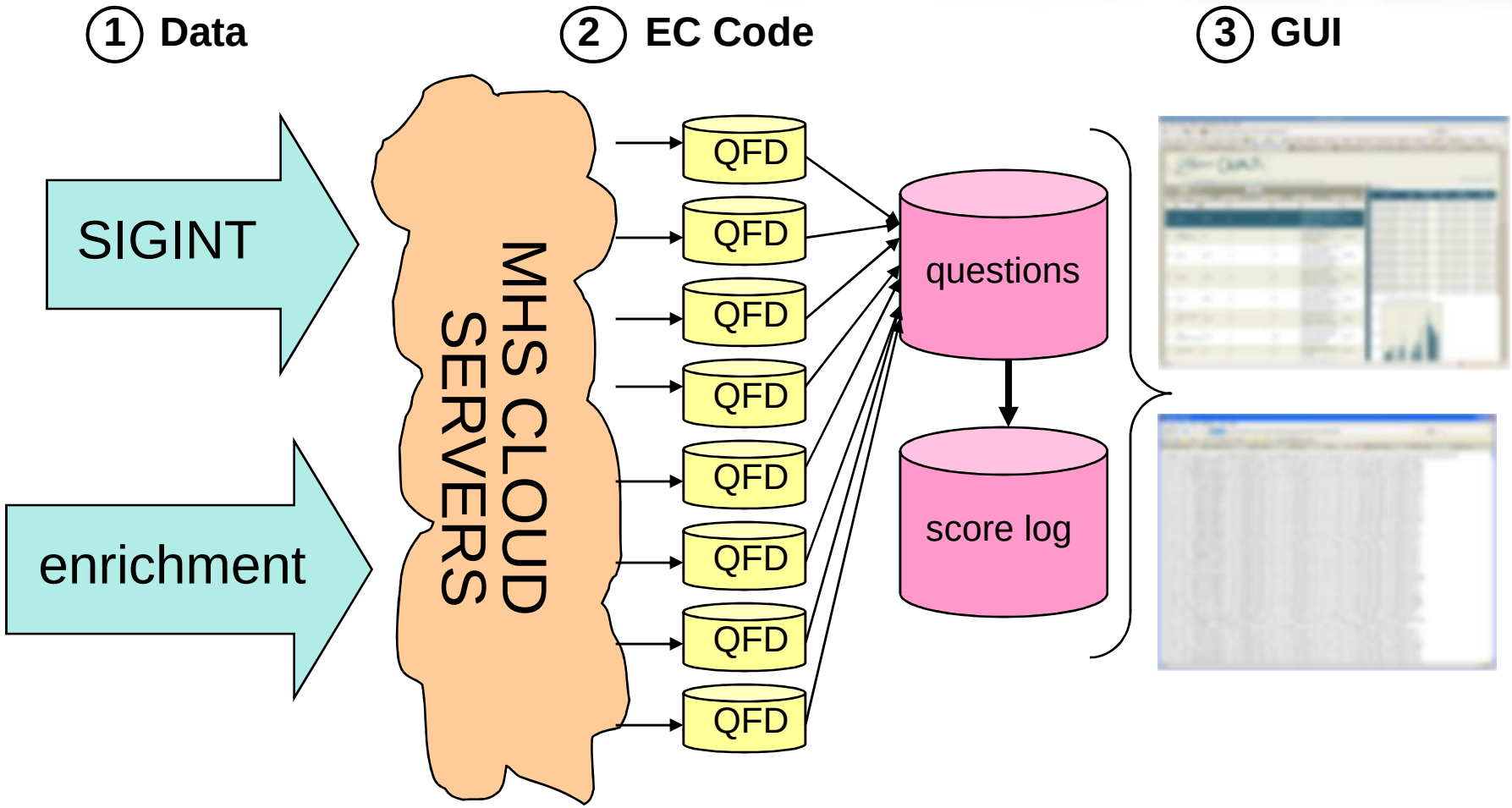
The MHS Cloud provides an excellent platform for this project:

- data ingest, normalization, tagging
- access to SIGINT data from various processors, from sustained mission + survey
- access to a huge body of enrichment data
- processing, storage, and web-hosting
  - considering decoupling these parts…

ELEGANTCHAOS In Context



EC System Overview



MySql tables and code

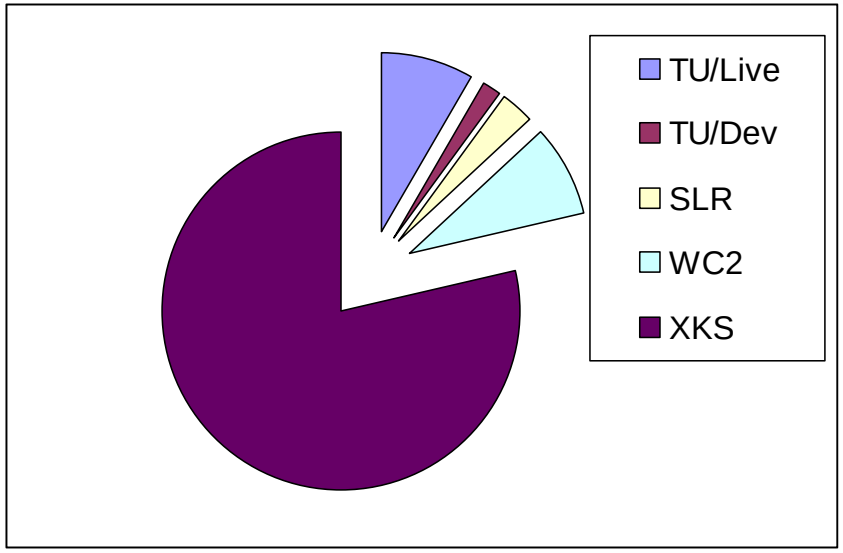
Data Sources (May 2011)

SIGINT Feeds

- XKEYSCORE
- ASDF (Turmoil LIVE)
- SLR (TARMAC)
- POPQUIZ (Turmoil DEV)
- WEALTHYCLUSTER2

Enrichment Feeds

- IPGeoTrap
- TRAVELLINGWAVE Scores
- BILBOBADGER Daily Summaries
- Target Network Service list + CNO Target list
- DRINKYBIRD monitoring info
- GLOBETROTTER OH Geo
- MASTERSHAKE Geo
- Quantumable Case Notation list



Event counts over a 12-hour period.

Total events: 335,663,981

Analytic Questions (May 2011)

Target

- Dictionary hits
- Target Networks
  - TNS, TW, CNO
- PLUS Reports, CRNs, etc.

Technology

- [redacted]
- VPNs
- Twitter, Facebook, VoIP
- CNO behavior

Location

- IP-based
- MAC-based
- Geo-based
- Surge Countries
  - Libya, Egypt, Afghanistan, Syria, Yemen, Ivory Coast, etc.

Miscellany

- Modem Capacity
- Paired Links
- Quantumable

Questions & Scoring

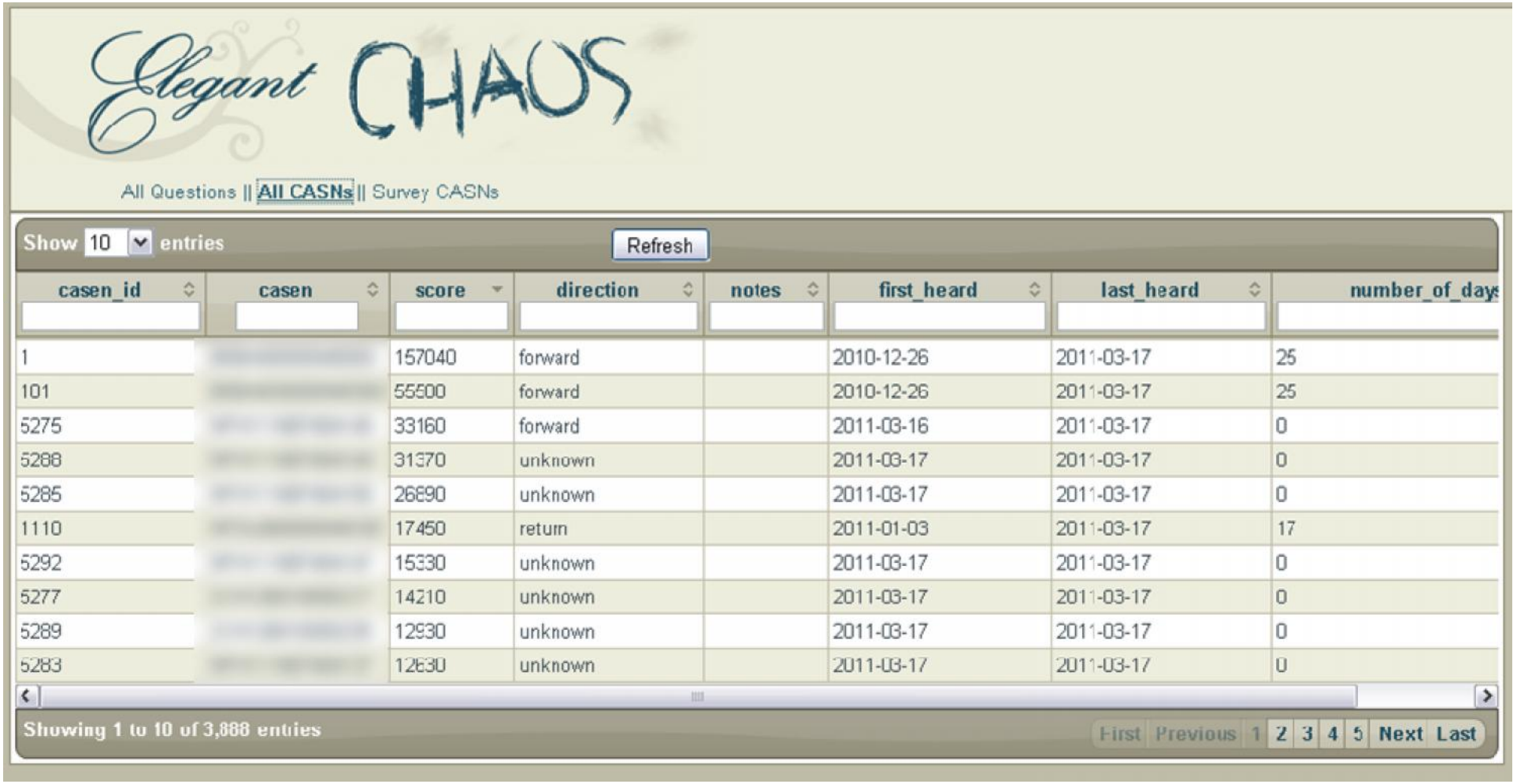
- Each question is represented by a SQL query applied to one or more QFDs
- QFDs are case notation-based repositories of signal information
  - eg, IPs and registries for all case notations
  - eg, category hits for all case notations
  - eg, GLOBETROTTER geos for all case notations
- All questions are asked once per day across all case notations
- Points are assigned to each question based on current analytic priorities
- Points for any particular question are “active” for a window of time (eg, 1 day, 7 days, 30 days)
- The sum of “active” points for a case notation, across all questions, forms the score

Interfaces

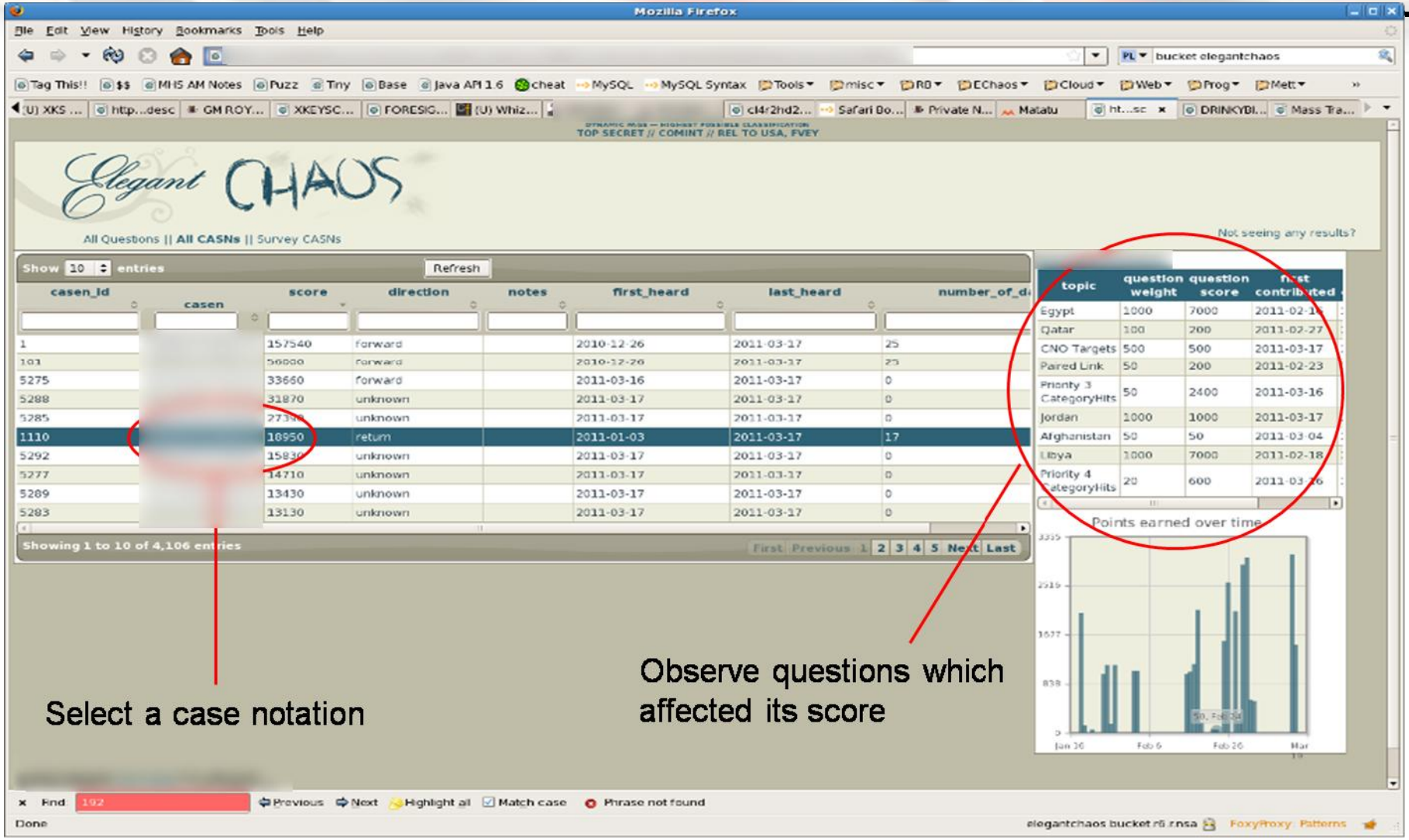
Different interfaces for different customers

- ELEGANTCHAOS GUI
  - made for analysts to examine scores and the impact of the different questions
  - eventually, control over the algorithms may reside here
- REST interface
  - made for programmatic query, precursor to auto tasking
- DRINKYBIRD GUI
  - made for collection personnel to determine if resources are available, easy to view what's on cover

EC GUI: Case Notation View



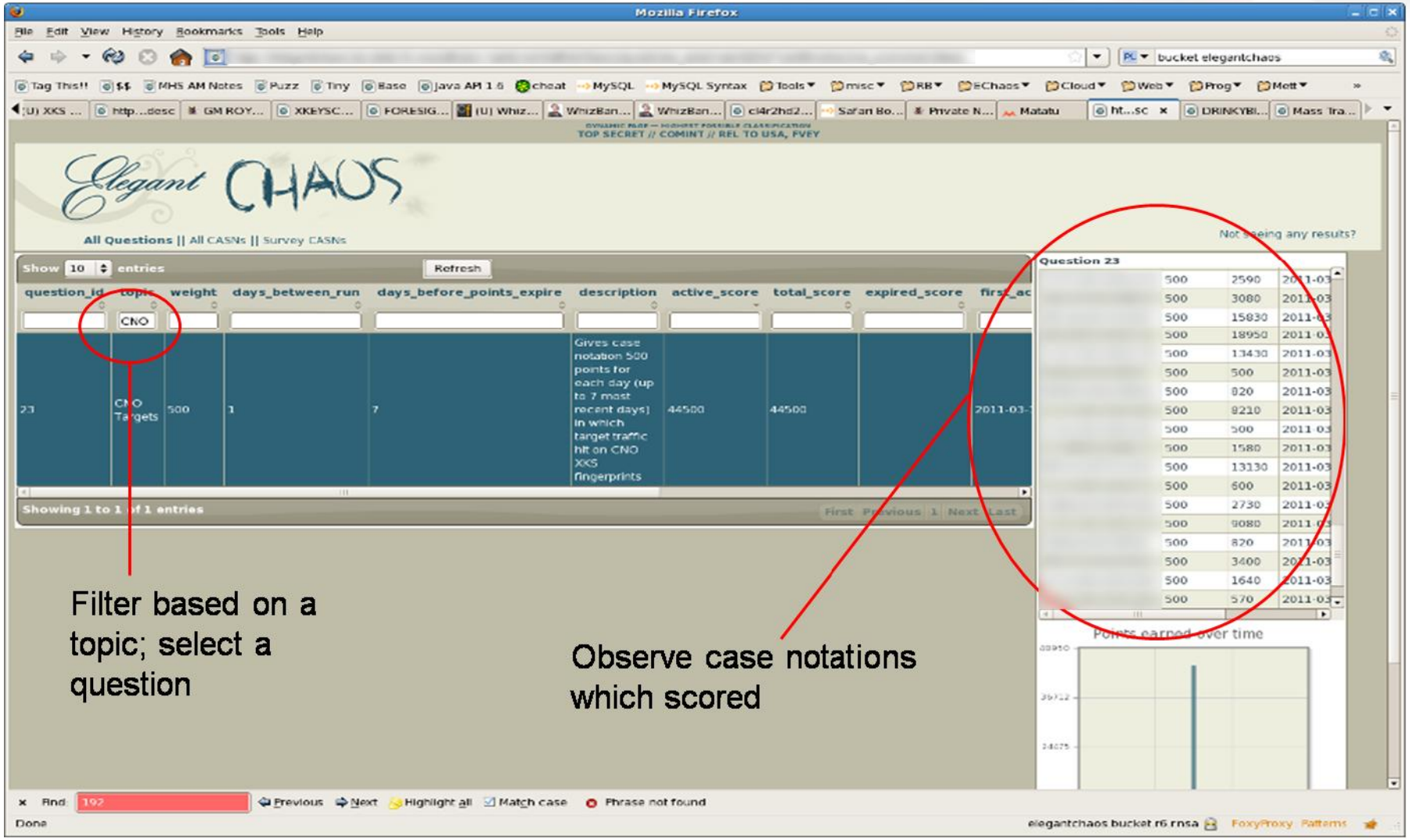
EC GUI: Case Notation View



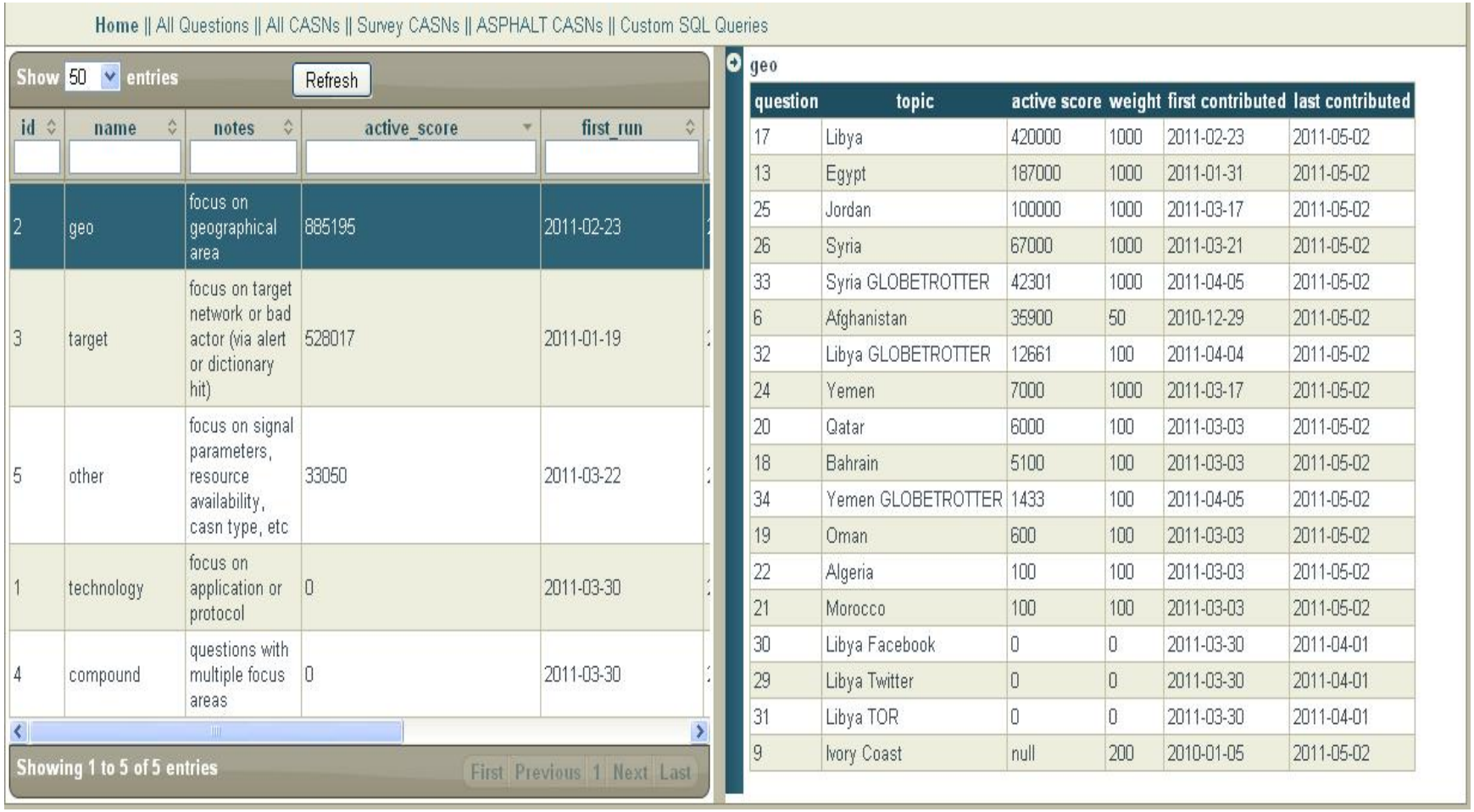
EC GUI: Question View

question_id	topic	weight	days_between_run	days_before_points_expire	description	active_score	total_score	expired_score	first_active_
15	[redacted]	1000	1	30	[redacted]	9000	15000	6000	2011 02 18
1	TRAFFICTHIEF I lit	1000	1	7	1000 points given each day for each case notation with a priority 1 (TRAFFICTHIEF) tip seen	28000	446000	418000	2011-03-15
17	Libya	1000	1	30	10000 points for each case notation with a Libyan IP address on the significant side of a link	117000	216000	99000	2011-02-17
13	Egypt	1000	1	30	Gives case notation 1000 points if the known signficantAQAT side of the link has an IP address that resolves to Egypt	62000	172000	110000	2011-02-16
14	FORNSAT CRNs	500	7	7	500 points for each casn with a current FORNSAT CRN	3[illegible]500	1825[illegible]00	1465[illegible]00	2011-03-15
12	Tasked Active Users	150	1	7	150 points given for a case notation if it has Marina Daily Active Counts greater than 0 in the BILBOBADGER Daily Summary	1350	16050	14700	2011-03-15

EC GUI: Question View



Focus Areas: Custom Views?



Home || All Questions || All CASNs || Survey CASNs || ASPHALT CASNs || Custom SQL Queries

Show 50 entries Refresh

id	name	notes	active_score	first_run
2	geo	focus on geographical area	885195	2011-02-23
3	target	focus on target network or bad actor (via alert or dictionary hit)	528017	2011-01-19
5	other	focus on signal parameters, resource availability, casn type, etc	33050	2011-03-22
1	technology	focus on application or protocol	0	2011-03-30
4	compound	questions with multiple focus areas	0	2011-03-30

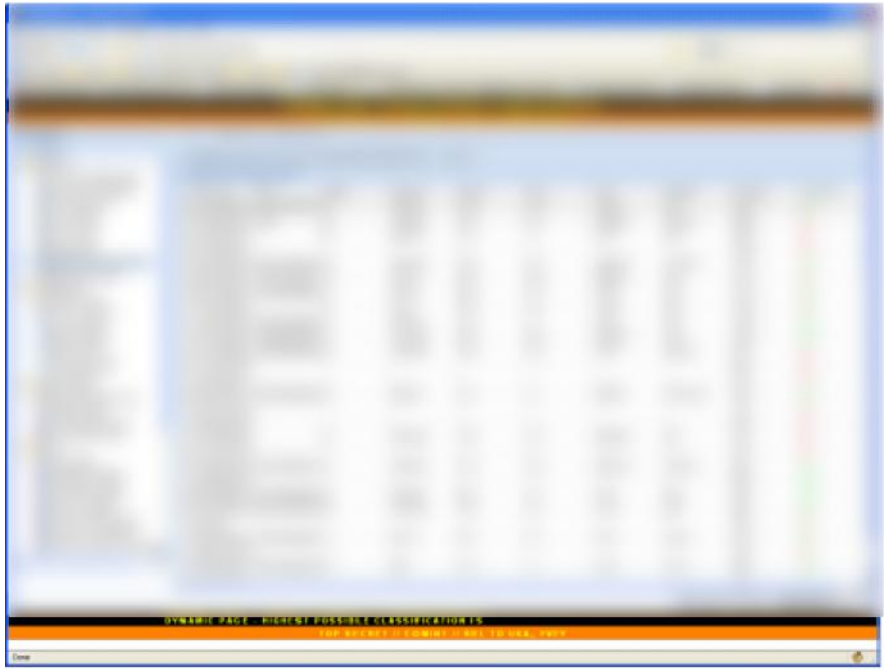
Showing 1 to 5 of 5 entries First Previous 1 Next Last

geo

question	topic	active score	weight	first contributed	last contributed
17	Libya	420000	1000	2011-02-23	2011-05-02
13	Egypt	187000	1000	2011-01-31	2011-05-02
25	Jordan	100000	1000	2011-03-17	2011-05-02
26	Syria	67000	1000	2011-03-21	2011-05-02
33	Syria GLOBETROTTER	42301	1000	2011-04-05	2011-05-02
6	Afghanistan	35900	50	2010-12-29	2011-05-02
32	Libya GLOBETROTTER	12661	100	2011-04-04	2011-05-02
24	Yemen	7000	1000	2011-03-17	2011-05-02
20	Qatar	6000	100	2011-03-03	2011-05-02
18	Bahrain	5100	100	2011-03-03	2011-05-02
34	Yemen GLOBETROTTER	1433	100	2011-04-05	2011-05-02
19	Oman	600	100	2011-03-03	2011-05-02
22	Algeria	100	100	2011-03-03	2011-05-02
21	Morocco	100	100	2011-03-03	2011-05-02
30	Libya Facebook	0	0	2011-03-30	2011-04-01
29	Libya Twitter	0	0	2011-03-30	2011-04-01
31	Libya TOR	0	0	2011-03-30	2011-04-01
9	Ivory Coast	null	200	2010-01-05	2011-05-02

REST: “Auto-tasking”

- ASPHALT
  - Updated list of prioritized casns



VENUSAFFECT

- Scores in DRINKYBIRD
- Using modem tasking sheet

DRINKYBIRD

Elegant Chaos tasking priority

Survey Casen	Casen	Satellite	Frequency	Polarity	Feed	Rasin	Data Rate	EC Priority	On Cover?
		BB	12551	VER	K3V	IDIRECTOC	19994.703	7300	no
		--	--	--	--	--	--	5000	no
		BB	12626.52	VER	K3V	IDIRECTOC	NaN	4350	no
		BB	12563.008	VER	K3V	WC1A	2048	4000	no
		--	--	--	--	--	--	3000	no
		BB	12653.745	VER	K3V	IDIRECTOC	--	3000	no
		--	--	--	--	--	--	3000	no
		--	--	--	--	--	--	2200	no
		--	--	--	--	--	--	2200	no
		BB	12658.442	VER	K3V	IDIRECTOC	7466.637	2000	no
		--	--	--	--	--	--	1200	no
		NF	12580.063	HOR	K3H	IDIRECTOC	4525.582	12600	yes
		2C	11501.069	HOR	K2H	IDIRECTOC	3780	8200	yes
		5B	12666.495	VER	K3V	DVBS	21000	7050	yes

Survey Casen	Casen

DRINKYBIRD – Tasking Priority View

EC Priority	On Cover?
7300	no

Libya Surge

PROBLEM

Which of the 1000's of signals surveyed have Libyan / Egyptian / Afghan networks on the VSAT-side?

SOLUTION

- Pre-run analytics determine "significance"
- Quick identification of 25 'LY' / 11 'EG' / 10 'AF' candidate signals
- Combine other analytics: target hits, pairing, etc.
- (Repeat for next country)

AMULET STELLAR

PROBLEM

Which case notations have traffic on IPs of interest that matches AST fingerprints?

SOLUTION

- Create IP target set; create whitelist and blacklist of XKS fingerprints
- Use Cloud capabilities to bridge between the set of all SIGINT events with matching fingerprints, and the target set
- Add the scoring question to EC

Ongoing Work

- New data feeds (FOGHORN, MATCHMAKER, ROADBED)
- More fields from XKS (HTTP language, NetStrings)
- XKS from MOONPENNY
- Fine tuning of GUI for Link Characterization Analysts
- NetStrings study
- *Better use of Cloud resources (Link Direction) (CCDP)*
- *Detailed study of scoring methodology (math hire)*
- *Close the auto-tasking loop (RSE)*
- Increase awareness and partnership with similar efforts
- Training

Questions?