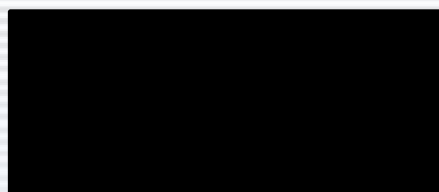


Identifier Lead Triage with ECHOBASE



NSA - S2I51
NSA - T1442

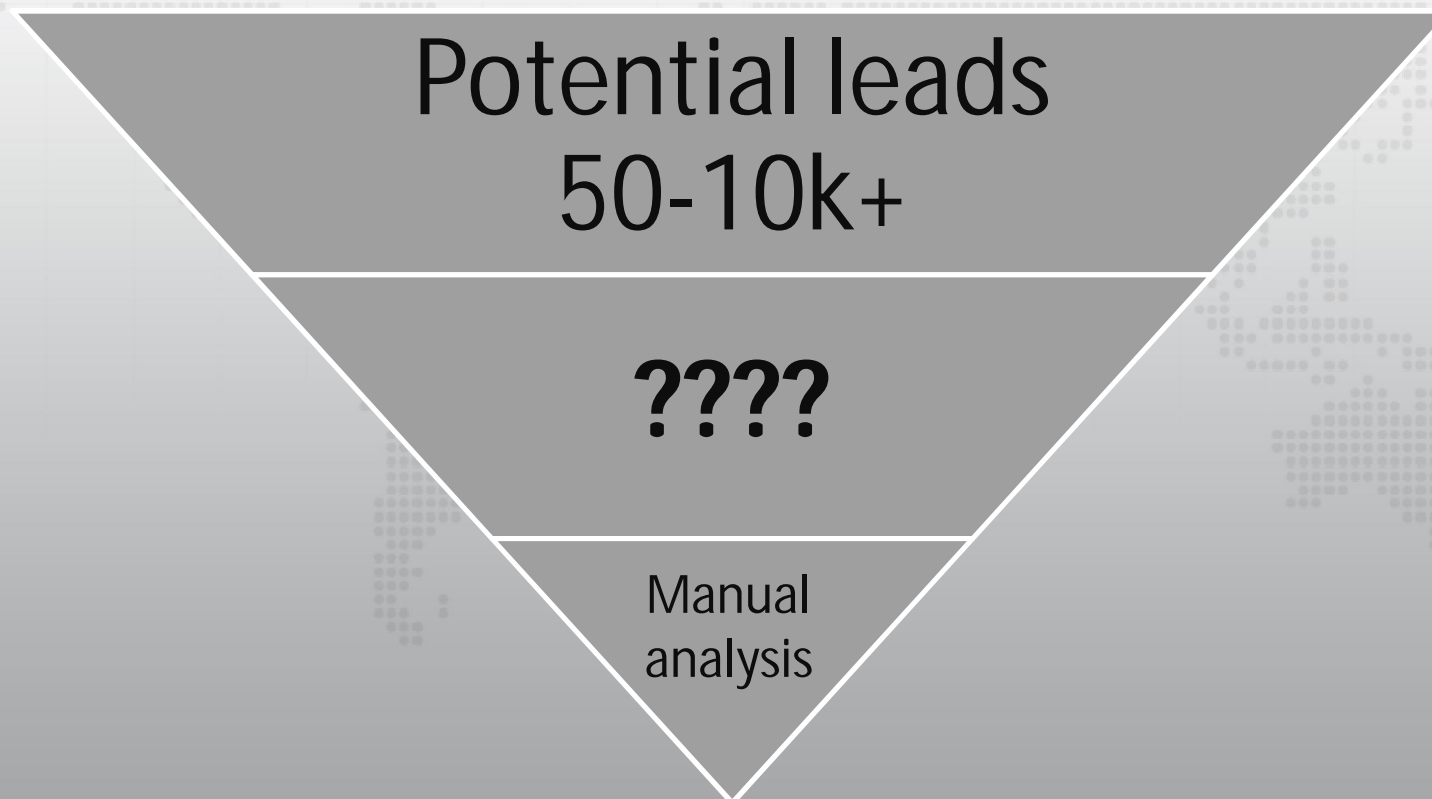
JUN 2012

The Problem



SIGINT is very good at 2 things:

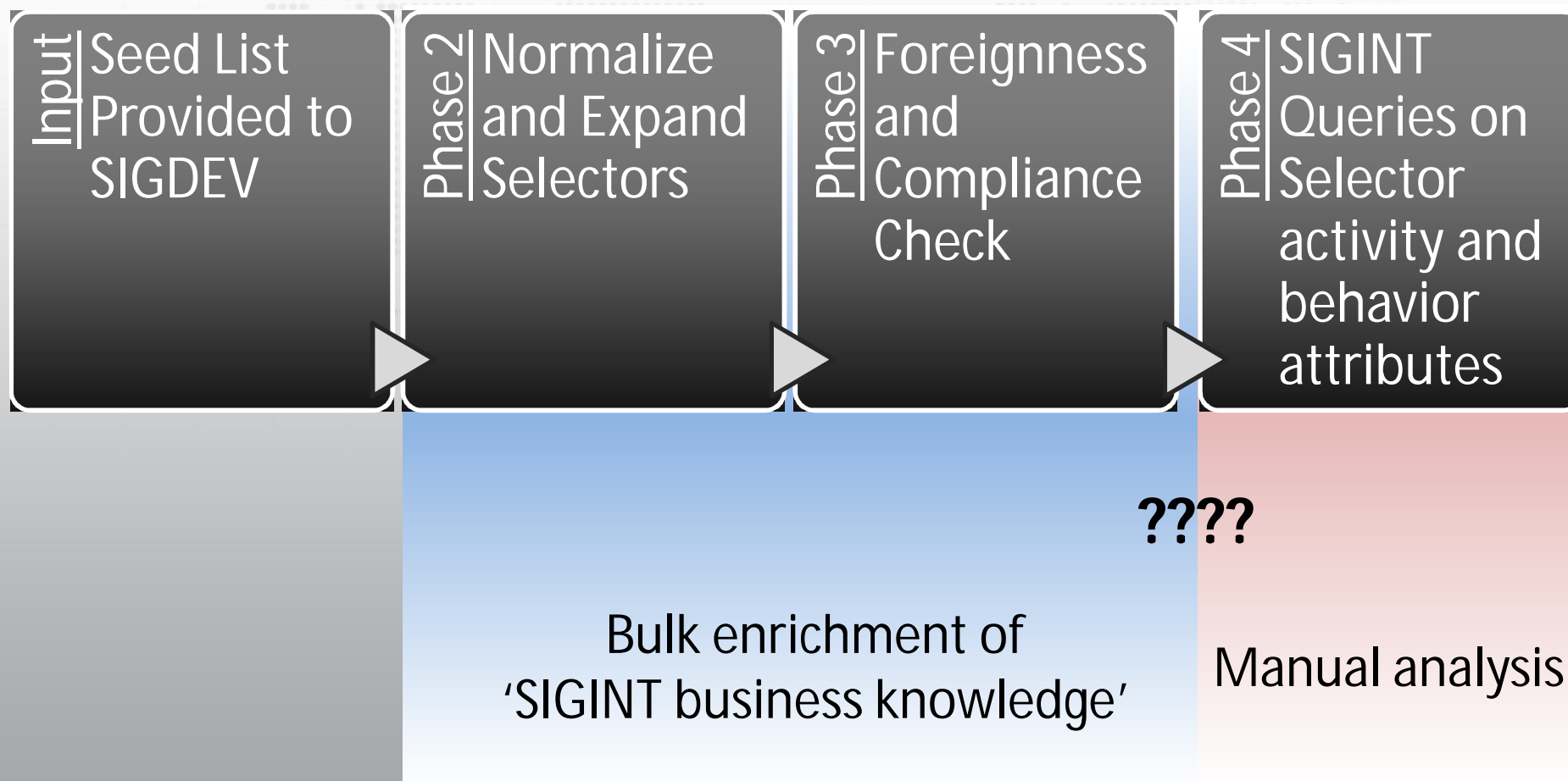
1. Establishing lists of potential leads (50-10k+)
2. Manual analysis to vet individual targets



Tradecraft



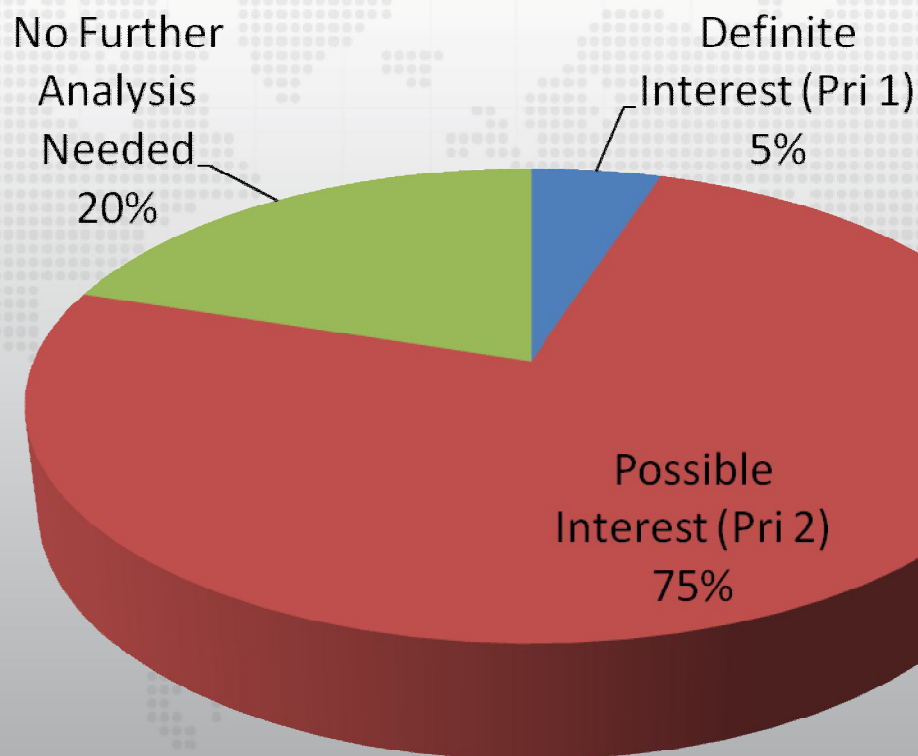
A common model for identifier lead lists, today:



Triage Today



After initial enrichment checks, the analyst is often left with too many identifiers of "possible interest"

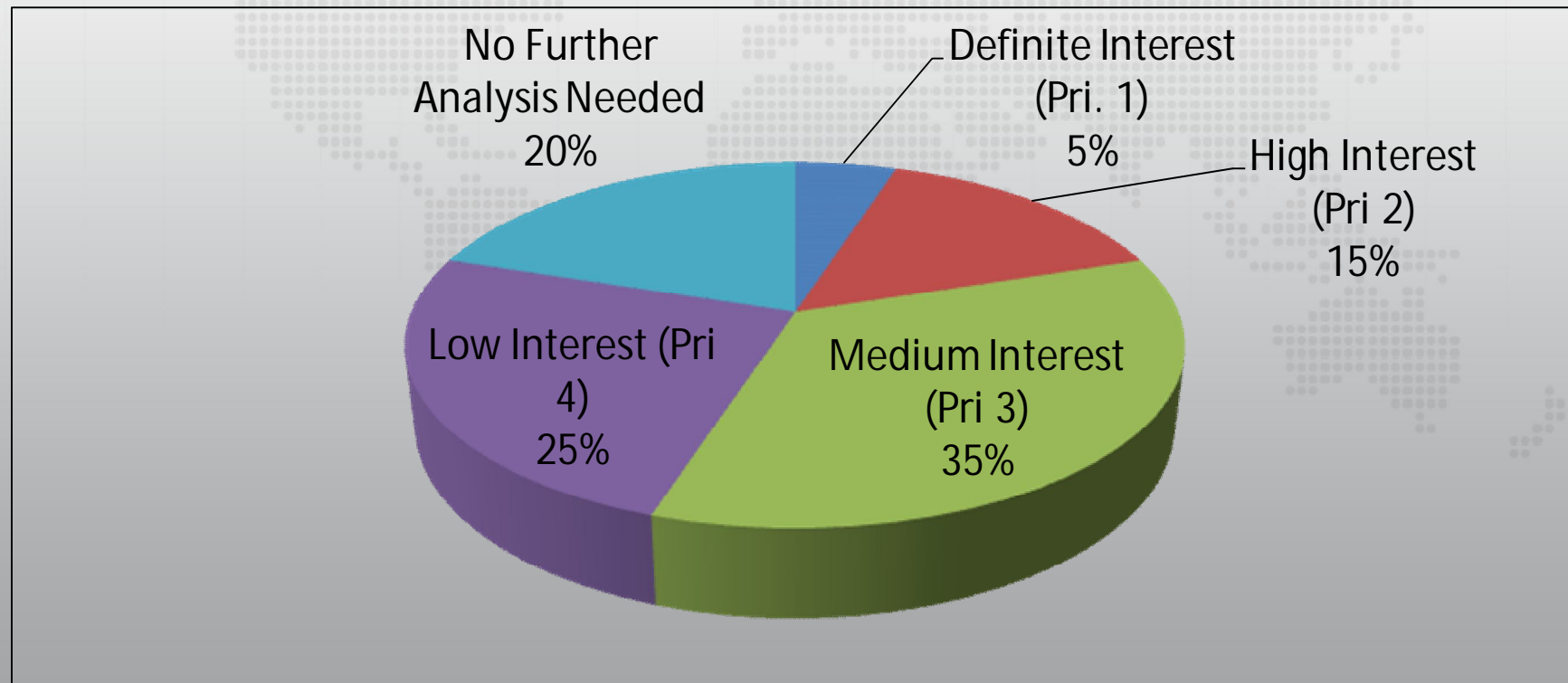


Percentages are conceptual

Bulk Lead Triage via Behavior Analytics



- Hundreds or thousands of selectors to go through high level vetting very quickly
- Better triage prioritization allows for highly adjustable thresholds to be set for follow -on analysis
- Compliance can be inserted at both the "batch result" and "query" level
- Potentially utilize multiple clouds & cross-enterprise analytics



Identifier 'SIGINT Business' Enrichment



Bulk gathering, via Identifier Scoreboard (phase 2/phase 3)

- Targeting
- Authorities
- Reporting
- Targets
- Knowledge
- Foreignness
- Compliance

*...not a raw
SIGINT query*

Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY

Identifier SCOREBOARD

Airport Threat

Hide lineup

Add identifiers

Change realm | Delete

Added	Context	Realm	
<input checked="" type="checkbox"/>	12147		x
<input checked="" type="checkbox"/>		yahoo	x
<input checked="" type="checkbox"/>	<skypeUser>	skypeUser	x

Validate =>

Import identifiers

Targeting tag: flag

Targeting category: []

Targeting zipcode: []

Query/criteria list: [] x
Priority Email [] x
Choose... []

Target: [] x
Choose... []

Retrieve up-to-date FOREMAN data Include correlations

Clear Save Search

Identifier view Target view

Create target Customize Send to...-

Normalized identifier	Targeting						Foreignness		Knowledge			Actions
	Comms	PSC	Tip	TAO	CNE	POCs	CONTRAOCTAVE	FOREMAN	Comments	Location	Reports	
[]						1	n/a	Unkown				
[]						1	n/a	Unkown			10	
[]						[] (S2I12)	n/a	Unkown				
[]						[] (F52)						
[]						4	n/a	Unkown	3			

Last updated: 2012-Mar-01 09:58:46 Z

Displaying 1-100 of 154 page 1 of 2

Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY

'Yes/No' Identifier Behavior



Bulk triage, via SIGINT Analytics Mode (start of phase 4)

Core set of 'yes/no' behavioral questions about a set of identifier leads

...against raw SIGINT!

Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY

About | Contact | A little help?

SIGINT

Airport Threat

Has this identifier been in direct communications with a targeted identifier?
 Identifiers supported: DNI and DNR
 Legal authorities: EO12333_S, EO12333_X, FAA_702_CP, FAA_702_CT, FAA_02_FG, FAA 704/705B
 Results updated: Daily
 more...

Identifier view Target view

Normalized identifier	Positive Results	Direct Comms with Target?	Targeted Contact?	In Captured Media?	Seen	Actions
[redacted]	2	•	n/a	n/a	n/a	[A] [G] [X]
[redacted]	n/a					[A] [G] [X]
[redacted] <msnpassport> View detailed analytic results	4	•				[A] [G] [X]
		Targets: [redacted] <yahoo> TP [redacted] <facebookname> TP First heard: 25 Oct 2011 Last heard: 09 Mar 2012			First heard: 03 Dec 2011 Last heard: 29 Feb 2012	[A] [G] [X]
[redacted] <yahoo>	3	•				[A] [G] [X]
[redacted] <emailAddr>	n/a					[A] [G] [X]
[redacted] <msnpassport>	4	•	•		•	[A] [G] [X]
[redacted] <facebookname>	2		•			[A] [G] [X]
[redacted] <skypeUser>	0					[A] [G] [X]
[redacted] <yahoo>	0					[A] [G] [X]
[redacted] <yahoo>	2	•				[A] [G] [X]
[redacted] <emailAddr>	2		•			[A] [G] [X]
[redacted] <msnpassport>	0					[A] [G] [X]
[redacted] <google>	0					[A] [G] [X]
[redacted]	0		n/a	n/a	n/a	[A] [G] [X]
[redacted]	2	•			•	[A] [G] [X]
[redacted]	4	•	•	•		[A] [G] [X]
[redacted]	7	•	n/a	n/a	n/a	[A] [G] [X]

Last ran on: 2012-Mar-01 09:58:46 Z

Displaying 1-100 of 148 page 1 of 2

(U//FOUO) Page Publisher: Identifier Scoreboard, T1422 | Content [redacted] T14 | Last Reviewed: 15-Dec-2010 | Last Modified: 23-Feb-2012
 (U//FOUO) Derived From: NSA/CSSM 1-52 | Declassify On: 20320108 | Dated: 08 January 2007

Dynamic Page - Highest Possible Classification is TOP SECRET//SI//REL TO USA, FVEY

SIGINT Analytics Mode



Triage by aggregate behaviors

Normalized Identifier	Positive Results	Direct Comms with Target?	Targeted Contact?	In Captured Media?		See
[+] [redacted]	2	•	n/a	n/a	n/a	
[+] [redacted]	n/a					
[-] [redacted] <msnpassport> View detailed analytic results	4	Targets: [redacted] <yahoo> TP [redacted] <facebookname> TP First heard: 25 Oct 2011 Last heard: 09 Mar 2012			First heard: 03 Dec 2011 Last heard: 29 Feb 2012	
[+] [redacted] <yahoo>	3	•				
[+] [redacted] <emailAddr>	n/a					
[+] [redacted] <msnpassport>	4	•	•		•	
[+] [redacted] <facebookname>	2		•			
[+] [redacted] <skypeUser>	0					
[+] [redacted] <yahoo>	0					
[+] [redacted] <yahoo>	2	•				
[+] [redacted] <emailAddr>	2		•			

One column per 'yes/no' question

Quickly zero in on worthy leads

SIGINT Analytics Mode – Detailed View



Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY

About | Contact | A little help?

SIGINT ANALYTICS

Analytic Results: [REDACTED] <msnpassport> 2012-Mar-01 09:58:46 Z

[View in Target Profiler](#)

Had direct communications with a targeted identifier?
[REDACTED]

Seen in captured media? (no results)

Seen in CNE? (no results)

Seen in France?

Seen on a targeted identifier's contact lists, or has a targeted contact? (no results)

▼ **Had direct communications with a targeted identifier?**
First heard: 2012-Mar-01 08:58:42 Z **Last heard:** 2012-Mar-05 07:55:40 Z

Date	Description	Source
2012-Mar-05 07:55:40 Z	[REDACTED] <msnpassport> cc'd email to [REDACTED] <yahoo>	UUID: [REDACTED] SIGAD/PDDG: DS-200A / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-04 09:58:46 Z	[REDACTED] <msnpassport> was bcc'd on email from [REDACTED] <msnpassport>	UUID: [REDACTED] SIGAD/PDDG: DS-200A / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-02 10:56:43 Z	[REDACTED] <msnpassport> received email from [REDACTED] <msnpassport>	UUID: [REDACTED] SIGAD/PDDG: DS-200B / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-01 08:58:42 Z	[REDACTED] <msnpassport> sent email to [REDACTED] <yahoo>	UUID: [REDACTED] SIGAD/PDDG: US-3171 / T8 Case notation: [REDACTED] Legal authority category: EO12333

[Back to top](#)

(U//FOUO) Page Publisher: Identifier Scoreboard, T1422 | Content [REDACTED] T14 | Last Reviewed: 15-Dec-2010 | Last Modified: 23-Feb-2012
 (U//FOUO) Derived From: NSA/CSSM 1-52 | Declassify On: 20320108 | Dated: 08 January 2007

Dynamic Page - Highest Possible Classification is TOP SECRET//SI//REL TO USA, FVEY

SIGINT Analytics Mode – Detailed View



▼ **Had direct communications with a targeted identifier?**
First heard: 2012-Mar-01 08:58:42 Z **Last heard:** 2012-Mar-05 07:55:40 Z

Date	Description	Source
2012-Mar-05 07:55:40 Z	cc'd email to	UUID: SIGAD/PDDG: DS-200A / C4 Case notation: Legal authority category: EO12333
2012-Mar-04 09:58:46 Z	was bcc'd on email from	UUID: SIGAD/PDDG: DS-200A / C4 Case notation: Legal authority category: EO12333
2012-Mar-02 10:56:43 Z	received email from	UUID: SIGAD/PDDG: DS-200B / C4 Case notation: Legal authority category: EO12333
2012-Mar-01 08:58:42 Z	sent email to	UUID: SIGAD/PDDG: US-3171 / T8 Case notation: Legal authority category: EO12333

[Back to top](#)

Go view target knowledge

Go view content

Add new knowledge

External links to guide next steps in analysis

ECHOBASE Analytics Architecture

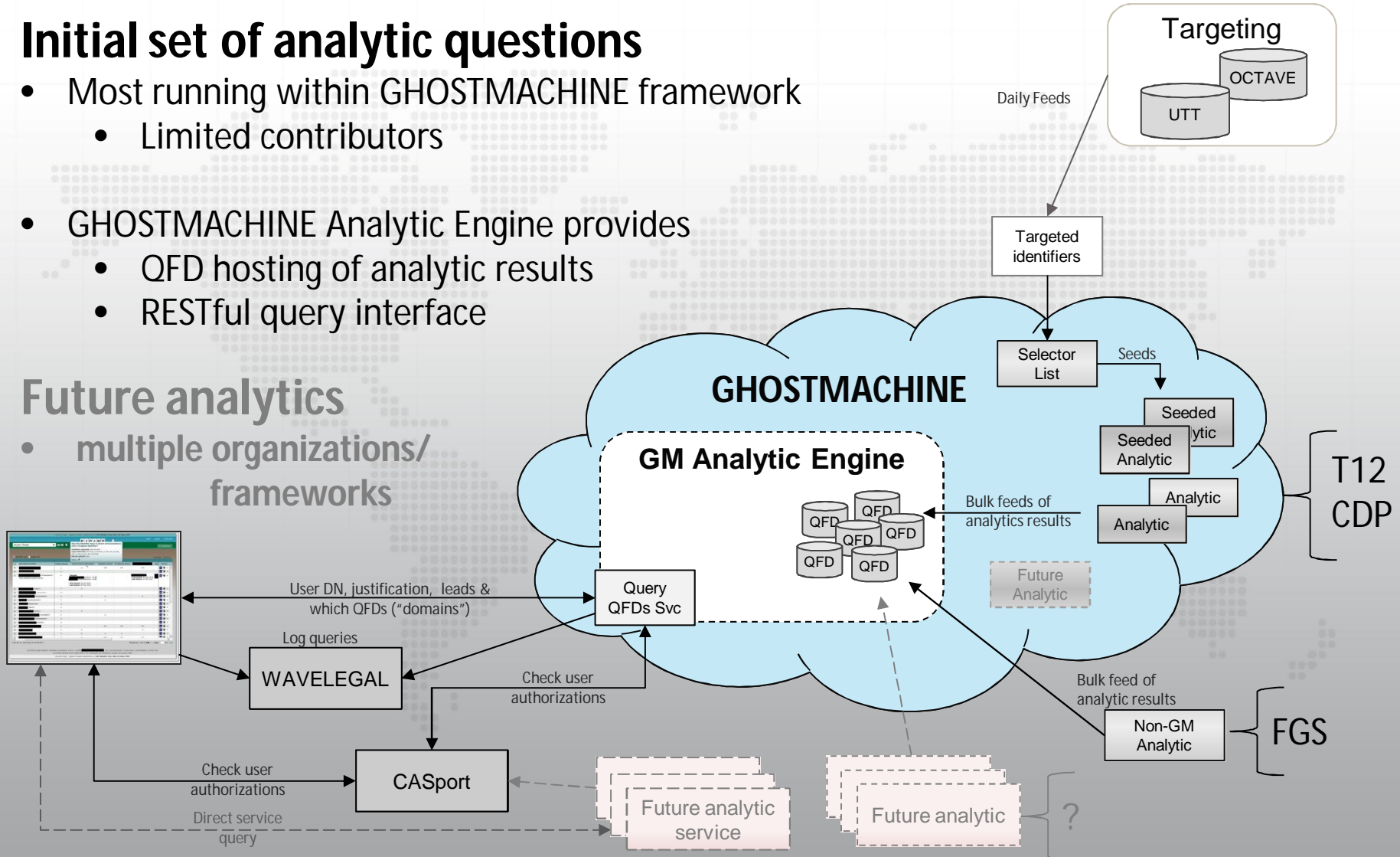


Initial set of analytic questions

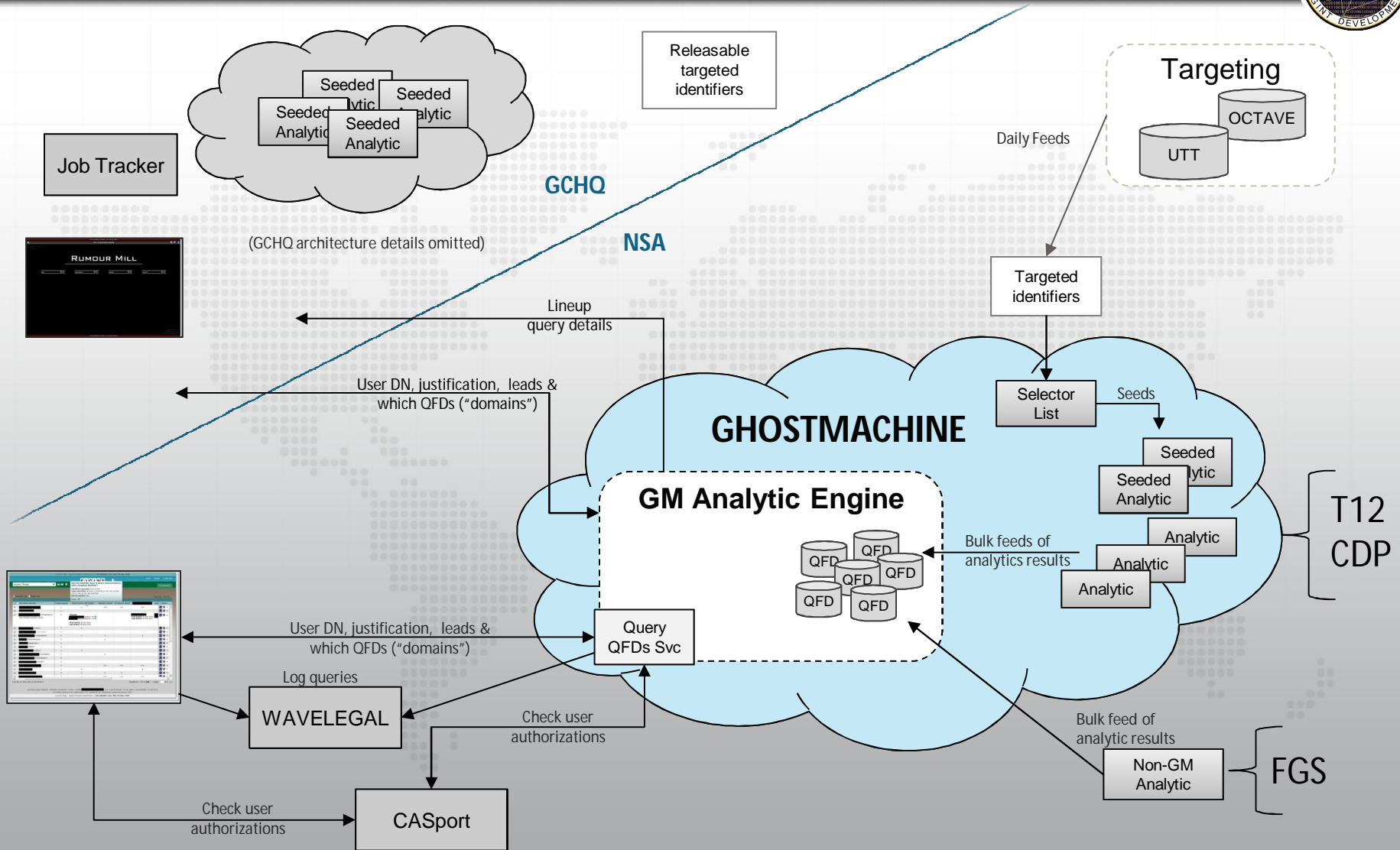
- Most running within GHOSTMACHINE framework
 - Limited contributors
- GHOSTMACHINE Analytic Engine provides
 - QFD hosting of analytic results
 - RESTful query interface

Future analytics

- multiple organizations/ frameworks



2012 Olympics Sharing



2012 Olympics Support



- NSA SID Leads Evaluation Cell
 - Triage of Olympics-based leads through the event
 - Leverage both NSA and GCHQ-produced analytics
- Greater SID-wide usage following the Olympic period

Contact/Information



- Briefers:

- [REDACTED]
- [REDACTED]

- ECHOBASE Alias:

- [REDACTED]

- NSA WikiInfo page:

- [REDACTED]