Events Product Centre
Agenda

- Welcome
- Immingle
- Salamanca
- QFDs
- Guiding Light
- Questions
Key changes July 2010 to present:

- Inferred data from B3M now flagged
- Updates to handle identifiers from HARD ASSOC and B3M correctly
- MAINWAY: MSRNs now grouped and flagged in same way as SALAMANCA
- MAINWAY: direct access to event details provided
- GPRS flagging – THUGGEE rules applied to SALAMANCA events
**events**

**IMMINGLE**

MAINWAY options and Help pages

SECRET STRAP1
GPRS flag and count

GPRS Events: 8

SAUDI ARABIA

MAINWAY II: 3, SALAMANCA: 3

SECRET STRAP1

GCHQ
What next?

- FASCIA GPRS flagging
- HAUSTORIUM decommissioning
- Next Gen Contact Chaining trial....
Key changes since July:

- NRT (Near Real Time) Storage = 3 days
- Extra feeds from TERRAINs at BUDE and SOUNDER
- 2nd Party usage of SALAMANCA: SHAREOWN replaces ESCHAR
- CallAnsweredState and CallEndState added to TERRAIN-SALAMANCA feed
Pakistan NGN inferencing errors
Current scale

- There are 100 unique bearers feeding the BzS tools.
- Consistently averaging over 30 billion events per-day into the input buffer.
  - MB is loading over 10.5 billion
  - 6 months data retention for MB = 1,890,000,000,000 records and requires 400 TB.
  - Total storage of over one petabyte.
Future Scale

- Further 58 bearers by end of 2010
- An additional 40 bearers in Q1 2011.
  - MB will ingest over 20 billion events per day requiring one petabyte of storage.
  - Overall storage will increase to 2.5 petabytes.
- Scope scaling to 400 bearers.
infimi = MOT
KARKA POLK
MEMORY UOL
MUlùfJI h-u
Hi SAWyEL

Pi "Hi i-4vlKl|i«(*gy
i
i

1

ryi'F ni II»? TTl lyv* yim  iff
Btiyye v'ahoo-Y^Ciofis

i

I

k

Tielihlwiw I.It-111 in Villi"'' V-

1

flihl»

SOCIAL fitiLMAL

JOCIAL MJThfiOroil

TDFM.ìii^v
shoo-V-L:ackJE
fyim  "DI
fifraj)» |Jspr
De-scityiinir-is  ìih  u&-name urine  vaino!  i. serene  slftagec  n.THeu»m3nne
is ine Irati  il :tin?  «haaiB-r>iall  tiiireis  {evefyfMfig  u^ittfie  •  If
citar  i* "ir  » [vimary domain- ;

Minar.- ifir.al.-i^c-  9S99R9SS
Pull through and upscaling of TR SPs.

- Currently 43 bearers.
  - 14 from TR SP
  - 29 additional bearers from TPS (generating HTTP, TDI, Websearch, FTP and Squeal).
  - Circa 40 additional bearers just generating Squeal.

- Approval to increase aperture to 100 bearers for all data-types.
- Approval to increase user numbers to 200.
SOCIAL ANTHROPOID
What is Social Anthropoid?

- SOCIAL ANTHROPOID is a converged comms database. It will allow you to see when your targets have communicated via phone, over the internet, or using converged channels (e.g., sending e-mails from a phone or making voice calls over the internet).
What about the existing comms databases?

- When SOCIAL ANTHROPOID contains all the necessary data and has all the core functionality of the legacy tools Social animal, HAUSTORIUM and SALAMANCA will be de-commissioned.
What data is in Social Anthropoid??

- All of Salamanca data (telephony)
  - Social animal data.
  - Instant Messenger.
- Webmail. - SIP & H323 VOIP
  - Yahoo Voice
  - Blackberry
    - MMS
- SMS (from Salamanca and other sources)
  - GTP (GPRS session set-ups)
    - And more..
What about SMTP, POP3 and IMAP?
- Starting to receive these data types now.
- Capability deployed as part of HeartBeat 11.
• Queries will be automatically submitted to all instances of SOCIAL ANTHROPOID, SOCIAL ANIMAL and Convergec SOCIAL MINIMAL.

• For bulk queries, enter multiple selectors (one per line).

• If allow wildcards is enabled, it is treated as a multi-character wildcard (e.g., paul.* will match paul123, paul156, paul@eagle.com vs. will match paul123@eagle.com but NOT paul123@gmail.com). Unlike other QEDs, and I have no special meaning to query for literal and/or or check allow wildcards rather than escaping the wildcard.

• By default, results will be returned in which your input selector appears in either the User A or User B column (in SOCIAL ANIMAL terms is the 'editor' or the 'subject' with the event). To return results in which your selector appears only as the active user, box the Query active users only checkbox.

• Front-end processing normalizes QED selectors in various ways, including the removal of dots from the usernames of email addresses. To get Gmail results, you will need to normalize your queries in the same way (e.g., search for bad@eagle@gmail.com instead of bad.eagle@gmail.com). Gmail also ignores the dots so there is no danger of getting events for the wrong account. If in doubt, consult your local QED tech.

Search period (option):
Filter results by matched selectors prior to display:
 Allow inactive:
Query active users only:

Miranda

CIC Priority & Purpose

HRA Justification

SECRET STRAP1
### Results Summary

<table>
<thead>
<tr>
<th>Action</th>
<th>Action Type</th>
<th>User A Role</th>
<th>User A Name</th>
<th>User A Type</th>
<th>User B Role</th>
<th>User B Name</th>
<th>User B Type</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>chat</td>
<td>message</td>
<td></td>
<td></td>
<td></td>
<td>message</td>
<td></td>
<td></td>
<td>02-Jul-2010 02-Jul-2016</td>
<td>24:01:19</td>
<td>14:01:29</td>
</tr>
<tr>
<td>chat</td>
<td>message</td>
<td></td>
<td>#REGION#@hotmail.com</td>
<td>email</td>
<td></td>
<td>#REGION#hotmail.com</td>
<td>email</td>
<td>23-Aug-2011 23-Aug-2011</td>
<td>15:34:16</td>
<td>15:34:16</td>
</tr>
<tr>
<td>chat</td>
<td>message</td>
<td></td>
<td>#REGION#hotmail.com</td>
<td>Sender</td>
<td></td>
<td>#REGION#hotmail.com</td>
<td>Unknown</td>
<td>23-Aug-2011 23-Aug-2011</td>
<td>15:34:16</td>
<td>15:34:16</td>
</tr>
<tr>
<td>chat</td>
<td>message</td>
<td></td>
<td>#REGION#hotmail.com</td>
<td>Sender</td>
<td></td>
<td>#REGION#hotmail.com</td>
<td>Unknown</td>
<td>23-Aug-2011 23-Aug-2011</td>
<td>15:34:16</td>
<td>15:34:16</td>
</tr>
<tr>
<td>chat</td>
<td>message</td>
<td></td>
<td></td>
<td></td>
<td>message</td>
<td></td>
<td></td>
<td>23-Aug-2011 23-Aug-2011</td>
<td>15:34:16</td>
<td>15:34:16</td>
</tr>
<tr>
<td>chat</td>
<td>message</td>
<td></td>
<td></td>
<td></td>
<td>message</td>
<td></td>
<td></td>
<td>23-Aug-2011 23-Aug-2011</td>
<td>15:34:16</td>
<td>15:34:16</td>
</tr>
</tbody>
</table>

**SECRET STRAP1**
### Telephony in Santhropoid

#### Events

<table>
<thead>
<tr>
<th>User A role</th>
<th>User A Type</th>
<th>User A</th>
<th>User A raw value</th>
<th>User A display name</th>
<th>User B role</th>
<th>User B Type</th>
<th>User B</th>
<th>User B raw value</th>
<th>User B display name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**03-Nov-2010 12:34:20 — telephony event (global), 2 selectors, duration: 00:00:06**

- **Action event:**
  - **Selectors:**
    - unknown call
tel_number
  - **Action type:**
    - unknown
  - **Action:**
    - unknown

- **Locators:**
  - Source Point Code: 10741
  - Destination Point Code: 20062

---

**03-Nov-2010 13:34:19 — telephony event (global), 2 selectors, duration: 00:00:06**

- **Action event:**
  - **Selectors:**
    - unknown call
tel_number
  - **Action type:**
    - unknown
  - **Action:**
    - unknown

- **Locators:**
  - Source Point Code: 10741
  - Destination Point Code: 20062

---

**03-Nov-2010 14:34:29 — telephony event (global), 2 selectors, duration: 00:00:06**

- **Action event:**
  - **Selectors:**
    - unknown call
tel_number
  - **Action type:**
    - unknown
  - **Action:**
    - unknown

- **Locators:**
  - Source Point Code: 10741
  - Destination Point Code: 20062
**Convergence - GTP tunnel**

<table>
<thead>
<tr>
<th>User A role</th>
<th>User A type</th>
<th>User A</th>
<th>User A raw value</th>
<th>User A display name</th>
<th>User B role</th>
<th>User B type</th>
<th>User B</th>
<th>User B raw value</th>
<th>User B display name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Details:**
- **Action:** create tunnel
- **Action Type:** tunnel
- **create tunnel:** imsi
- **create tunnel:** tel_number
- **create tunnel:** blackberry_mid_pma

**Locators:**
- **Source IPv4:** 192.168.1.10
- **Source SqnAddress:** 1
- **Destination IPv4:** 192.168.1.20

**Event Details:**
This event represents the creation of GTP tunnel.

**View all events from this GTP tunnel**
Convergence – Leaky Gateways

### Table

<table>
<thead>
<tr>
<th>User A role</th>
<th>User A type</th>
<th>User A</th>
<th>User A display name</th>
<th>User B role</th>
<th>User B Type</th>
<th>User B</th>
<th>User B raw value</th>
<th>User B display name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Secret Strap1**
<table>
<thead>
<tr>
<th>User A role</th>
<th>User A type</th>
<th>User A</th>
<th>User A raw value</th>
<th>User A display name</th>
<th>User A email</th>
<th>User B role</th>
<th>User B type</th>
<th>User B</th>
<th>User B raw value</th>
<th>User B display name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SECRET STRAP1
Looks good, When can I have an account?

- Santhropoid is currently in the second stage of UAT.
- We currently have 200 users representing all areas of the business.
- Aiming to be in a position to release Santhropoid to the masses in early January.
<table>
<thead>
<tr>
<th>New data sources</th>
</tr>
</thead>
</table>

- **LUSTRE** – new data-source available in MB. Good for North Africa.

- **Source field** – This will enable new non-routine data-sources to be added to the QFD’s.
  - CNE
  - JTRIG – GLASSBACK data used for test case.
  - COLLATERAL
New loaders deployed to MB and HR Map, improvements to KP.

- Latency of the data in the QFDs has been greatly reduced, now around 12 hours.
  - Each instance of MB can now ingest 8 billion events per-day (total 32 billion)
- Some QFDs were previously 1-5 days behind.
- Query performance during loading has also been improved.
GUIDING LIGHT QFD

Presented by (Guiding Light SU)
What is GUIDING LIGHT?

New QFD developed in August 2010 by TDB-Events.

Primary objective:

“To understand the traffic seen on the Next Gen Events bearers.”
What can it do for me?

General Questions:
- Given a case notation, what are the TDI types that are found on it?
- Given a TDI type/subset, which bearers produce the highest number of events?
- What type of traffic is on which bearers and where is it coming from?
- Which bearers provide the most amount of traffic type x from place y?
GUIDING LIGHT

From Date
Custom 01-NOV-2010

To Date
Custom 01-NOV-2010

Bearer e.g. GWUKC151%

Event Type e.g. %facebook%

Country Digraphs (using ISO standard)

Query Type Country A Country B
From A to B

Min Event Count

Note. The % wildcard character represents 0 or more characters.

Daily Counts Source Types Bearers Countries Event Types Full Profile

SECRET STRAP1
### Results - Full Profile Query

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Source Group</th>
<th>Count</th>
<th>Source Type</th>
<th>Count</th>
<th>Count</th>
<th>Reference Count</th>
<th>Count</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event 1</td>
<td>Group 1</td>
<td>100</td>
<td>Event Type 1</td>
<td>50</td>
<td>20</td>
<td>10</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>Event 2</td>
<td>Group 2</td>
<td>200</td>
<td>Event Type 2</td>
<td>100</td>
<td>50</td>
<td>20</td>
<td>20</td>
<td>200</td>
</tr>
<tr>
<td>Event 3</td>
<td>Group 3</td>
<td>300</td>
<td>Event Type 3</td>
<td>150</td>
<td>75</td>
<td>30</td>
<td>30</td>
<td>300</td>
</tr>
</tbody>
</table>

SECRET STRAP1
## Event Types

### Results Pivot: Event Types

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo-B-Cookie</td>
<td>3,370,673</td>
</tr>
<tr>
<td>Yahoo-Y-Cookie</td>
<td>2,682,201</td>
</tr>
<tr>
<td>WEBSITE</td>
<td>2,519,571</td>
</tr>
<tr>
<td>SIP-INVITE From</td>
<td>874,568</td>
</tr>
<tr>
<td>HOST_REFERER</td>
<td>439,609</td>
</tr>
<tr>
<td>YM3G</td>
<td>364,400</td>
</tr>
<tr>
<td>SIP</td>
<td>345,876</td>
</tr>
<tr>
<td>Yahoo-Messenger</td>
<td>337,035</td>
</tr>
<tr>
<td><a href="http://www.google.com.pk">www.google.com.pk</a></td>
<td>14,485</td>
</tr>
<tr>
<td>Google-PREFIX-0okie</td>
<td>71,337</td>
</tr>
<tr>
<td>Simbar-SIMBAR-User-Agent</td>
<td>38,747</td>
</tr>
<tr>
<td>EXP_Shoppe:reports-SRS_IT-User-Agent</td>
<td>33,847</td>
</tr>
<tr>
<td>Facebook-c_user-Cookie</td>
<td>21,664</td>
</tr>
<tr>
<td>Yahoo-SIP-REGISTER-From</td>
<td>16,444</td>
</tr>
<tr>
<td><a href="http://www.bing.com">www.bing.com</a></td>
<td>14,485</td>
</tr>
<tr>
<td>clients1.google.com.pk</td>
<td>14,093</td>
</tr>
<tr>
<td>SIP-REGISTER-From</td>
<td>14,020</td>
</tr>
<tr>
<td>Yahoo-B-Sel-Cookie</td>
<td>11,720</td>
</tr>
<tr>
<td>Google-PREFIX-0okie</td>
<td>10,107</td>
</tr>
<tr>
<td>Yahoo-Y-Sel-Cookie</td>
<td>8,631</td>
</tr>
<tr>
<td>MS-MUID-Cookie</td>
<td>7,222</td>
</tr>
<tr>
<td>Yahoo-login-Method-Body</td>
<td>6,964</td>
</tr>
<tr>
<td>Google-Earth-Tile</td>
<td>6,905</td>
</tr>
</tbody>
</table>
Events

Results Pivot: Countries (From)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>CH</td>
<td>410</td>
</tr>
<tr>
<td>US</td>
<td>DE</td>
<td>341</td>
</tr>
<tr>
<td>US</td>
<td>GB</td>
<td>290</td>
</tr>
<tr>
<td>US</td>
<td>FR</td>
<td>167</td>
</tr>
<tr>
<td>US</td>
<td>IT</td>
<td>102</td>
</tr>
<tr>
<td>US</td>
<td>TP</td>
<td>98</td>
</tr>
<tr>
<td>US</td>
<td>SI</td>
<td>72</td>
</tr>
<tr>
<td>US</td>
<td>TR</td>
<td>67</td>
</tr>
<tr>
<td>US</td>
<td>IL</td>
<td>44</td>
</tr>
<tr>
<td>US</td>
<td>JP</td>
<td>17</td>
</tr>
<tr>
<td>US</td>
<td>CA</td>
<td>17</td>
</tr>
<tr>
<td>US</td>
<td>IN</td>
<td>12</td>
</tr>
<tr>
<td>US</td>
<td>NL</td>
<td>9</td>
</tr>
<tr>
<td>US</td>
<td>SE</td>
<td>9</td>
</tr>
<tr>
<td>US</td>
<td>BR</td>
<td>6</td>
</tr>
<tr>
<td>US</td>
<td>TW</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>AU</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>SE</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>ZA</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>JP</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>TR</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>SE</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>TP</td>
<td>1</td>
</tr>
</tbody>
</table>

SECRET STRAP1
Recent Enhancements

- Data from Bude (RPC)
  - Including data from SWORDDPLAY

- New fields
  - PDDG
  - SIGAD
  - SSDG
Future Enhancements

Near future:
- Adding BROAD OAK Targeting data
- Incorporating MI functionality from REFORMER (where appropriate!)
- Adding more feeds. (Ongoing)

Longer term:
- Adding Cipher and eAD MI information
- Linkage into ARTEMIS (or its successor)