QFDs and BLACHOLE
Technology behind GCHQ/INOC

March 2009

© This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on

Slide 1
'BLACK HOLE'

Probes -> Flat Store -> Analytic engines

- 10G
- Multi
- <10G

Question specific DBs (INOC today)
Data-mart extraction
MESME/Netezza etc.

Clouds

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

UK SECRET STRAP2 COMINT ORCON
BLACK HOLE

- Flat data store – not a database
- ~1,100,000,000,000 events since 6th August 2007
  - 53.3TB compressed
  - 217TB uncompressed
  - 47% of data is from last 3 months
- ~10 Billion events per day
- Cheap system:
  - £1k per TB of storage
  - £20k per 10Gbps probe
  - ~£400k for 10x10Gbps prototype

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act. Information may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.
Questions – INOC Today

Who, Where, When, What? – Online presence (TDI)

- MUTANT BROTH

Who, which website(s)? – Online browsing activity

- KARMA POLICE

Who, which fora? – Bulletin board usage

- INFINITE MONKEYS

Where? – Google maps/earth usage

- MARBLED GECKO
Questions – INOC Today

Who, Where, When, What? – Online presence (TDI)

Who, which website(s)? – Online browsing activity

Who, which fora? – Bulletin board usage

Where? – Google maps/earth usage

… And many more
Questions – INOC Today

Too many specific questions… Too much for analysts to learn.

Need analyst systems to be **simple** and **intuitive**.

Let analysts find & simply understand their targets easily…

drill in to systems only when they need to
Number of users who executed > 10 queries, by area