XKeyscoreTabs XKS Development

Jump to: navigation, search

News	Getting an Account	Using XKeyscore	Training	XKS Development	XKS Contacts	Requirements	News Archive

Contents

Quick Links

- XKEYSCORE Main Page
- XKS @ scale on SSE
- Getting Strong-Selected Content into XKS
- Getting an XKS Account
- Using XKEYSCORE
- XKEYSCORE Training
- **XKEYSCORE Development**
- XKEYSCORE Contacts
- XKS News Archive
- XKS Requirements
- XKS Searches user guide
- XKS Results user guide
- XKS Approval process
- NFV in XKS
- Promotion from XKS
- Automatic Promotion from XKS
- XKS for CNE
- NSA XKeyscore Using XKS for CNE
- XKS Tech Dictionaries

Useful Links

- Mastering The Internet
- Transforming Analysis
- TINT
- GTE
- SD Home

v · d · o

[edit] XKS Upgrades

XKS is upgraded fortnightly on Thursday mornings between 0900-1100. If you can't log on or use the tool during this period, its because of this.

[edit] Guidance on microplugins

As you know, you can create microplugins to do different things: some perform advanced detection techniques to find types of traffic which can't be detected by keywords or regular expressions alone. Others identify and extract data fields into XKS's metadata table.

In the latter case, the extracted content fragments are stored in the metadata table for 30 days. It will depend on the precision and nature of the search criteria you have used as to how strongly – or weakly – selected that content will be.

If you are going to use search criteria that will extract data about people and store that in the metadata table, please consult OPPLEG before doing so. They will wish to understand the nature and scope of any data being stored in case it includes at least the names of individuals and the majority of the data is not believed to relate to probable intelligence targets. This would make this data particularly sensitive.

In addition, a quarterly check is now being made on all new microplugins which add data to the

metadata table to ensure they meet UK legal and policy requirements.

Please also be aware that usually microplugins are automatically shared with at least NSA and may also get deployed lo other 2P XKS. By mid-2011 a new version of XKS should have been deployed where individual microplugins will still be deployed lo every XKS, but they can be tagged not to run on certain XKS. The only exception is where you deploy a microplugin only to GTE's XKS fleet: these will not be visible to 2P partners.

[edit] Types of XKEYSCORE

There are currently three different types of XKS:

- **Traditional**
- **Stage 2**
- **Deep Dive**

They differ principally on where in the processing chain they sit, whether the data they receive has already been sessionised or not and whether they ingest all of the data they receive or whether they apply rules to only ingest some data.

[edit] Traditional

When XKS was first developed it was used to receive data from low data rate signals being processed through WEALTHYCLUSTER (WC). WC sessionised all the data on the link and presented it all to XKS. All data was ingested into XKS.

GCHQ has traditional XKS at many of our sites, including all of our Comsat, Terrestrial and SMO sites. The EREPO XKS is also a traditional XKS, though in that case data has been softly selected at the implant and sessionisation takes place in TERRAIN, rather than WC.

[edit] Stage 2

For higher data rates, a "Stage 2" XKS was developed to ingest data from TURMOIL. TURMOIL passes 5% of the packets to XKS which XKS then sessionizes. TURMOIL decides which 5% of packets to pass based on the following criteria:

- strong selection
- subnet promotion
- technology promotion
- e-mail domains
- persona session promotion (where if a strong selector is seen, 10 minutes' or 10 MB of data is collected)
- persona session collection (where the data is collected and forwarded to NSA's PINWALE but is also passed to the XKS)

This data is then sent lo the Stage 2 XKS. All other data is lost.

Only JPC (MUSCULAR) at GCHQ uses a Stage 2 XKS.

[edit] Deep Dive

Deep Dive XKS was developed to prove that sessionisation at 10G data rates was possible. First it sessionises all data on a link. Then it promotes data using the GENESIS selection language to identify data types where we assess there is potential intelligence value and ingests those. The promotion process can make one of three decisions:

- Block data that is legally not allowed to be in the system – ie UK-UK traffic
- Allow data that is known to be wanted through use of promotion rules
- And then to drop any data that doesn't meet either of these

One of the experiments in TINT is seeking to identify where the best balance lies between what is kept and what is not. A factor in deciding how much data to keep is the scale of storage capacity that can be provided.

GCHQ already operates a number of Deep Dive XKS: