TWO FACE

From GCWiki
(Redirected from TWOFACE)
Jump to: navigation, search

Small gold ndist logo.jpg

Mtilogo cyberdef whitebg.gif

Logon to PALANTIR OPERATIONAL
Logon to PALANTIR REF
Logon to FRACTAL JOKER
Logon to FRACTAL WEB
Logon to PENSIVE GIRAFFE
Logon to LIVE
Logon to XKEYSCORE Viewer

Contents

[edit] Vision

"To Drive forwards the mission for effective Analysis and Knowledge use for Cyber Defence by providing more efficient complex analysis and sharing of knowledge"

[edit] Targets

Next Deliveries will be:

1. Automation of XKS importer
2. Improve flexible importing of data
3. Improved QFD Helpers (in no order): AutoAssoc / Social Anthropoid / Infinite Monkeys / Karma Police.
4. Improve UI performance and look and feel

[edit] 5 Eyes Collaboration

- CD Target DSD Palantir
- DSD-GCHQ Palantir Tests
- SE diagram of the GCHQ - DSD Palantir Link up
- Cyber Defence Targeting

[edit] Documents

See Palantir Documents or Online Instance

[edit] How to Guides ...

These are now starting to be generated so ideas are gratefully received.

1. Getting started
    1. How do I...Get Started in Palantir
    2. How do I...Use the different entities in Palantir
    3. How do I...Get the accounts I need and set up a development environment (DISCOVER link)
2. Importing X-KEYSCORE into Palantir
    1. How do I...Get Data from XKS in Palantir
    2. How do I...Select an XKS profile for importing my data
    3. How do I...Start an XKS search from Palantir
    4. How do I...Find which end is the server in Palantir **NEW**
3. Working with data from QFDs
    1. How do I...Run Sam Pepys queries in Palantir
    2. How do I...Run HrMap queries in Palantir
    3. How do I...Run Mutant Broth queries in Palantir
    4. How do I...Associate Mutant Broth Presence Events with HRMap Request events in Palantir
4. Working with the Graph view
    1. How do I...See an auto preview of a document or object properties? **NEW**
    2. How do I...Label objects with additional Properties using Bulk Object Editor **NEW**
    3. How do I...View lists of objects **NEW**
    4. How do I...View lists of objects with a given type or Property **IN PROGRESS**
    5. How do I...Change object type **NEW**
    6. How do I...Work with large groups in Palantir
    7. How do I...Rapidly find specific Properties in the Histogram **IN PROGRESS**
5. Publishing Data
    1. How do I...Publish in Palantir **NEW**
6. Find and view data within Palantir
    1. How do I...Find the Signatures in Palantir
    2. How do I...Use RT Tickets In Palantir
    3. How do I...Use the Histogram to filter events in Palantir
    4. How do I...Get a different view on existing events data in Palantir
    5. How do I...Rapidly view large numbers of events in the Browser **NEW**
7. Searching
    1. How do I...Run a bulk search
8. Miscellaneous
    1. How do I...Run bulk operations over my objects in Palantir
    2. How do I...Copy data from Palantir into Excel or Word **NEW**

[edit] Overview

This page details the datasources currently available within Palantir as well as other sources of data that are currently in development or planned. For current integration status, see the RTC project for TO120/144

[redacted]

Note that this page lists sources of data rather than helpers. For example, GEOFUSION HACIENDA and FOXTRAIL are all accessible through the same helper within Palantir.

[edit] Current datasources

Datasource	Import method	Under development?	Deployed to PIT?	Deployed to OP?	Notes
CROUCHING SQUIRREL	Auto-resync	No	No	Yes	
HALTER HITCH	Auto-resync	No	Yes	Yes	
GEOFUSION	Analyst-driven helper	Yes	Yes	Yes	
HACIENDA	Analyst-driven helper	Yes	Yes	Yes	
FOXTRAIL	Analyst-driven helper	Yes	Yes	Yes	
GORDIAN KNOT	Analyst-driven helper	No	No	No	GK Broke their PKI somehow; requires investigation
XKEYSCORE	Analyst-driven helper	No	Yes	Yes	
SAMUEL PEPYS	Analyst-driven helper	No	Yes	Yes	
MUGSHOT	Analyst-driven helper	Yes	No	No	
RAPID TAPIR	Analyst-driven helper	Yes	No	No	Deployment awaiting data owner OK
NTOC reports	Manual import by analysts	Yes	Yes	Yes	Automation to be investigated
FIVE ALIVE	Analyst-driven helper	No	No	Yes	
GOOGLE FUSION	Tiles for map application	No	Yes	Yes	
TO144-Notepit	Analyst driven external webpage	Yes	Yes	No	
Open source malware info	Auto-Resync	No	Yes	Yes	
INTEGER SPIN	Analyst-driven helper	Yes	Yes	Yes	
HRMAP	Analyst-driven helper	Yes	No	Yes	Too highly classified for PIT
NDIST RT	Auto-resync	Yes	No	No	Too highly classified for PIT
MUTANT BROTH	Analyst-driven helper	Yes	No	No	Too highly classified for PIT
OpenStreetMap	Tiles for map application	No	Yes	Yes	

[edit] Planned datasources

Datasource	Notes
DEAD SEA	API needs investigation
MOONRAKER/OBERON	Raptorable datasource
Open source data	TO144 open source data. Some integration work done.
8ball	Analytic value needs investigation. Some initial scripts written, not deployed anywhere
Global Surge	Highly nocon. Something to pass across to [redacted] in TDB?
DISCOVER	Lots of politics required
Oberon	Required for EPR. Needs further discussion with legal/policy

[edit] Project Details

[edit] Ontology

[1]

[edit] Contacts

Senior User: [redacted]

SE Lead: [redacted]

PM: [redacted]

Data Owner: [redacted]

Business Change: [redacted]

[edit] Training

Training is currently offered as 1-2-1 desk based training with a Palantir trainer. This gives you the opportunity to quickly apply Palantir to your current work task. If you would like to find out more about training please contact [redacted]

[edit] Task

As part of the Cyber Defence Theme, the strand that was searching for a Knowledge Storage tool. The results of the first part of this strand will be published shortly. As part of this process we determined that we really needed a bit of a kick forward in the technology we use. It was decided to trial Palantir to see what this could do for the business, and more specifically the Cyber Defence Mission. There is part of this strand to understand the gaps in our toolset. (more information here next week)

This page will develop fairly rapidly as we understand how we use the tool. Ontology comes first! (hence it takes up most of this page)

[edit] User Base

The User base is specifically for CDO and CDL. The Ontology, the data sources, the focus is purely for the Cyber Defence/Network Defence remit. The operationally used version will be locked via PKI to these individuals. However, the development section will have a slightly wider audience. There will be access for people wider than NDIST to help build the understanding throughout the organisation.

[edit] Logon

Logon site is: Palantir

[edit] Ontology

Needs more here... Or a link.

[edit] Requests and new requirements

Please email [redacted] for any new requests or requirements. Also worth contacting the Palantir SU [redacted] to explain the context and importnace of request.

[edit] Present Ontology

So as many of the analysts now can access the tool themselves, removing the duplication of having the ontology on the wiki.

[edit] Quick Questions

This is a quick set of notes on things I get asked a lot:

Is there an IM channel for us to chat informally? yes

> *There is a Jabber channel related to this topic:*
> ***palantir*** *- palantir-gchq + User informal chat)*

Are people outside NDIST going to get Palantir?

That's a question being answered by Transforming Analysis' CASK project. However, we're helping them by providing access to our

Sandbox server, so they can try it without affecting CDO's operational use.

I get a weird error and it won't open when I move desks?

Yes, this is due to desktop set-up. Return to the launch page, and start from there instead of your local icon.

Why do I have a bunch of burgundy coloured entities on my Graph?

These are the results of your last search around, if you do another search around they change to normal colours.

How does my team manage the results of our investigations?

Management of 'investigations' isn't really in Palantir (yet), we are talking with Palantir about producing a solution. At the moment you have to do an investigation of those investigations (if that makes any sense).

Why on import do I have loads of 'connections' as entities?

Well each of those connections is something you might care about, at the moment it starts at the most information and lets you decrease what you see (select all those connections and 'link merge' to get rid of them). When we smooth out the helpers we will give you the option to swap between 'entity' and 'property'.

Can I do some development in Palantir?

Sure, just give us a shout at palantir-support-dl about what you want to do and we will try and help.

I get an odd java error on startup (and there is a web-password issues here too)

Make sure you set your Java settings to: Network Settings > Automatic Proxy > [redacted]

My password doesn't work

On the operational box it's your Corporate Directory password.

But I'm not an NDIST user. What then?

Email palantir-support-dl

Category: Palantir

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted] [redacted] [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]