

- NDIST

THE TALE OF TWO SOURCES

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360501

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to



Rugby World Cup 2011.

- For the first time, we are all in it. 
- Last winners: South Africa. (they beat England).
- Starts 10th September in New Zealand.



A Guide to Rugby.

- This is a rugby ball. Note it looks a bit like American Football



- You pass the ball backwards:

Good



Bad



The Kit..

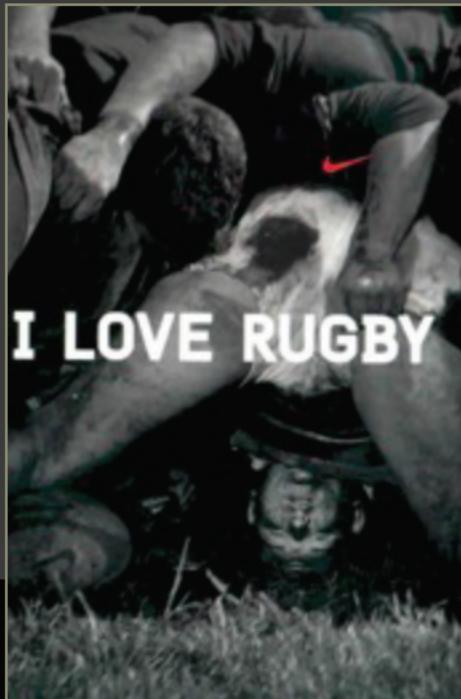
- Protection is allowed.



- Weaponry isn't!



It gets a bit..mucky.



It's a game for all



Not that American Football isn't:



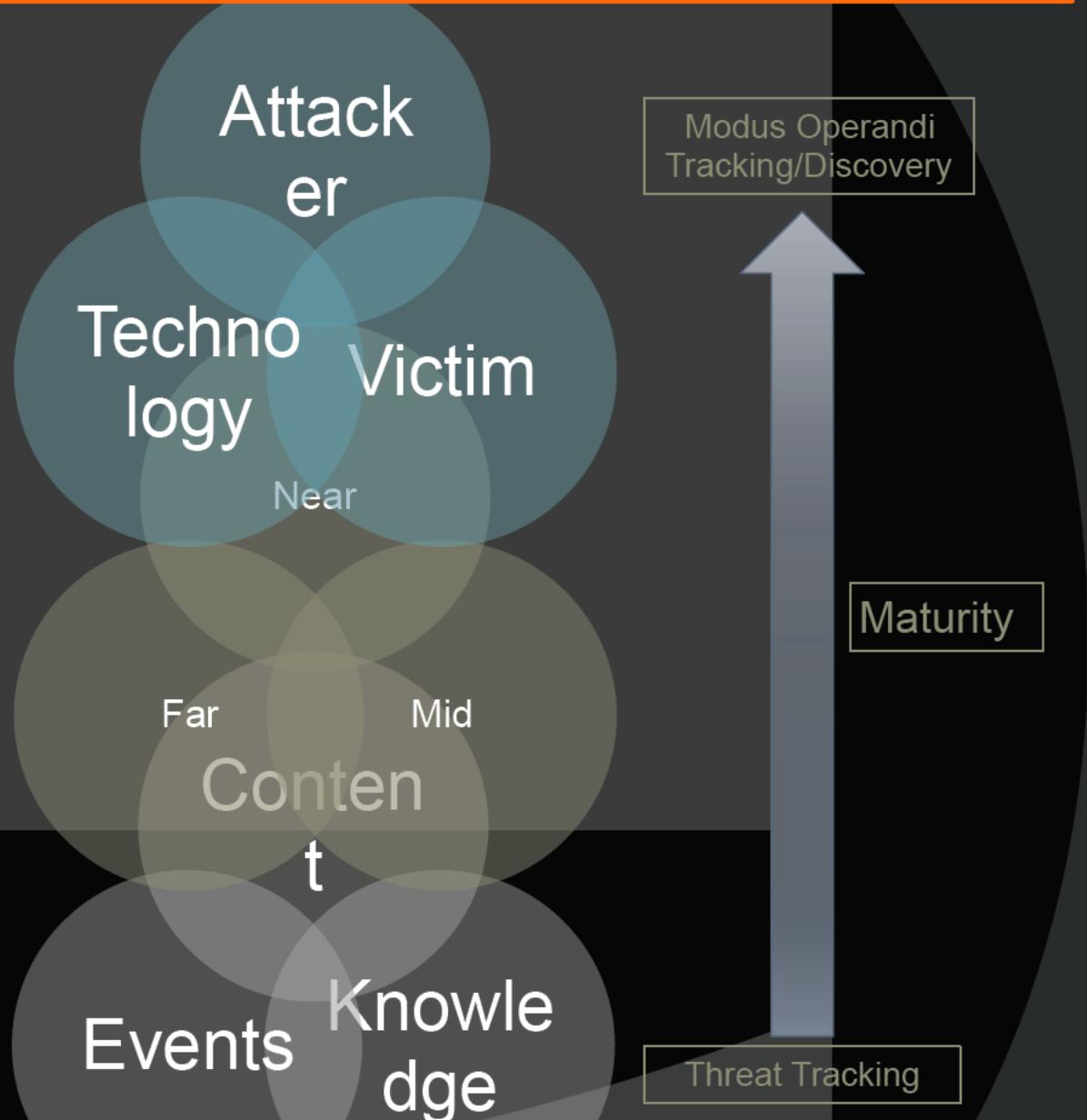
Business isn't usual!

- Unlike our agencies, the NZ'ers aren't small.

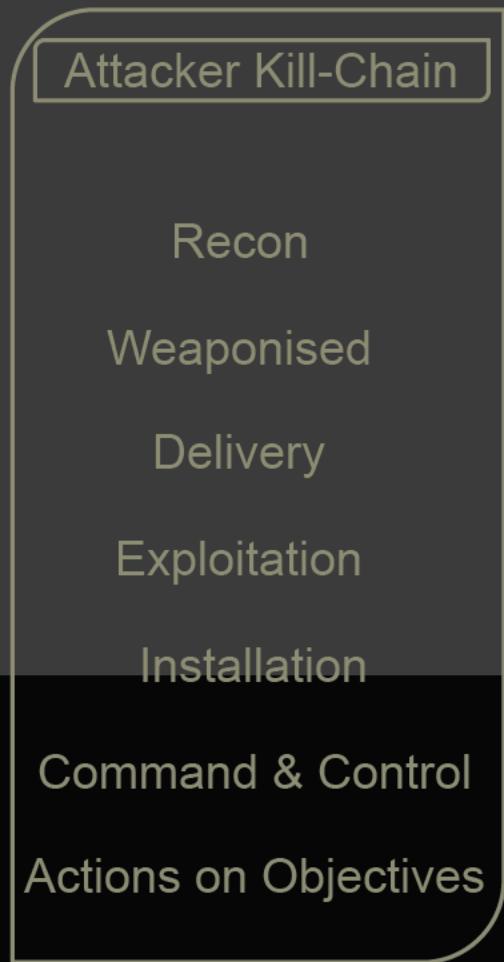


- And the Australians are successful 50% of the time!
- And the Chinese are not a threat.

The Goal



The Asymmetric Challenge

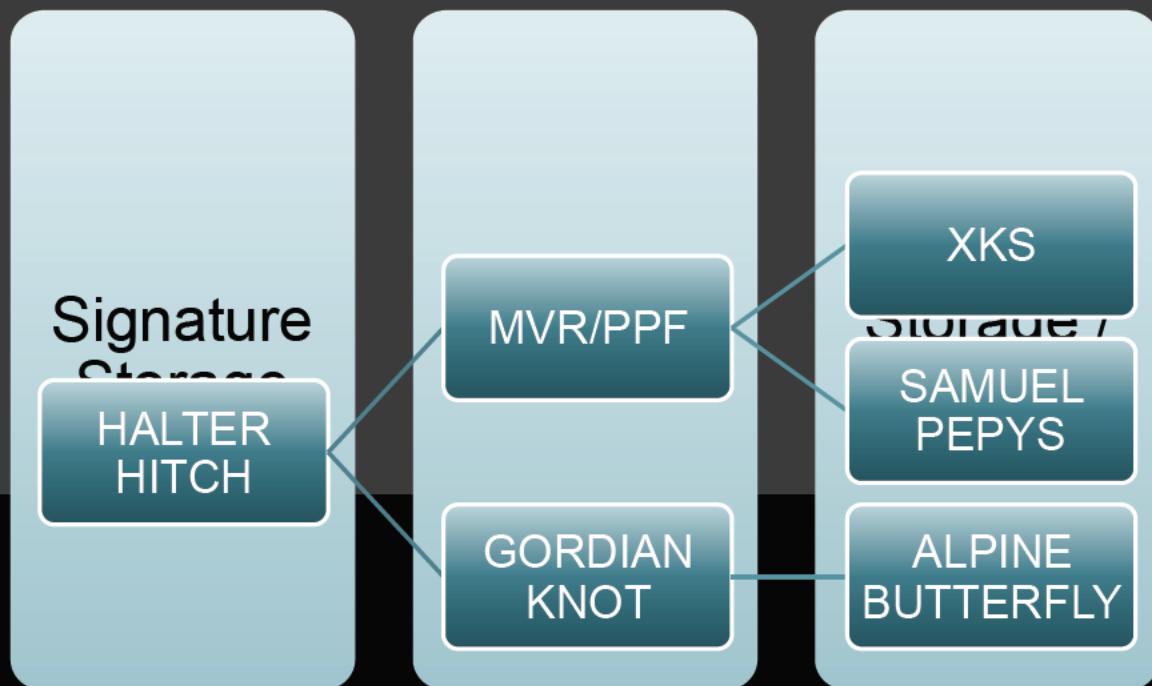


Far

Mid

May 2010

At the turn of the new Financial Year we had:



Far

Mid

Sigint Story

- Started at 13 x 10g Bearers
- Presently at 180 x10g Bearers

- From 1000 Signatures
- To 2500 Signatures

- Including Tryst and Comsat



nt

Events

Knowl
edge

Challenges ahead

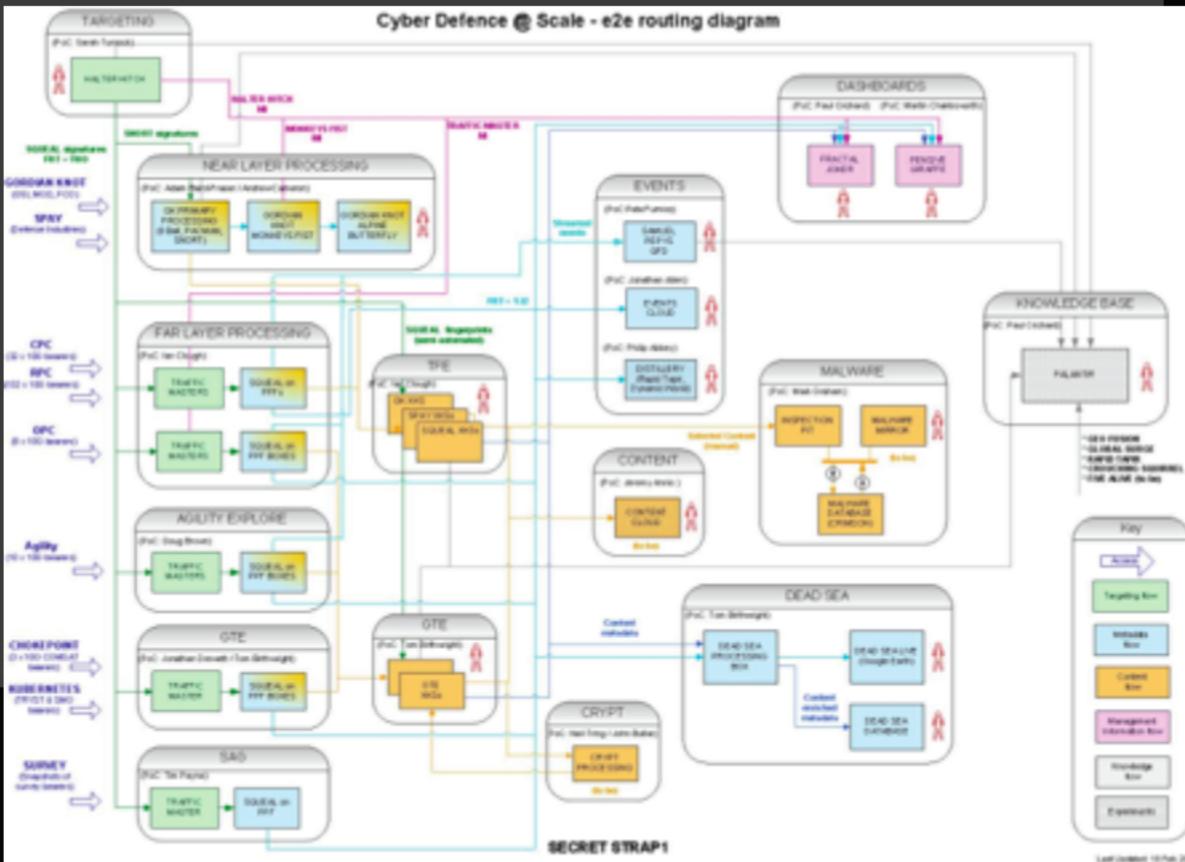
- Good collection, poor analytics.
- Focused on tracking.
- No status visualisation for end2end System.

nt

Events

Knowl
edge

What about the Sigint Collection?



What is the state of collection?

Signature Storage

Halter Hitch

MVR/PPF

GORDIAN KNOT

XKS

SAMUEL PEPYS

ALPINE BUTTERFLY

FRACTAL JOKER

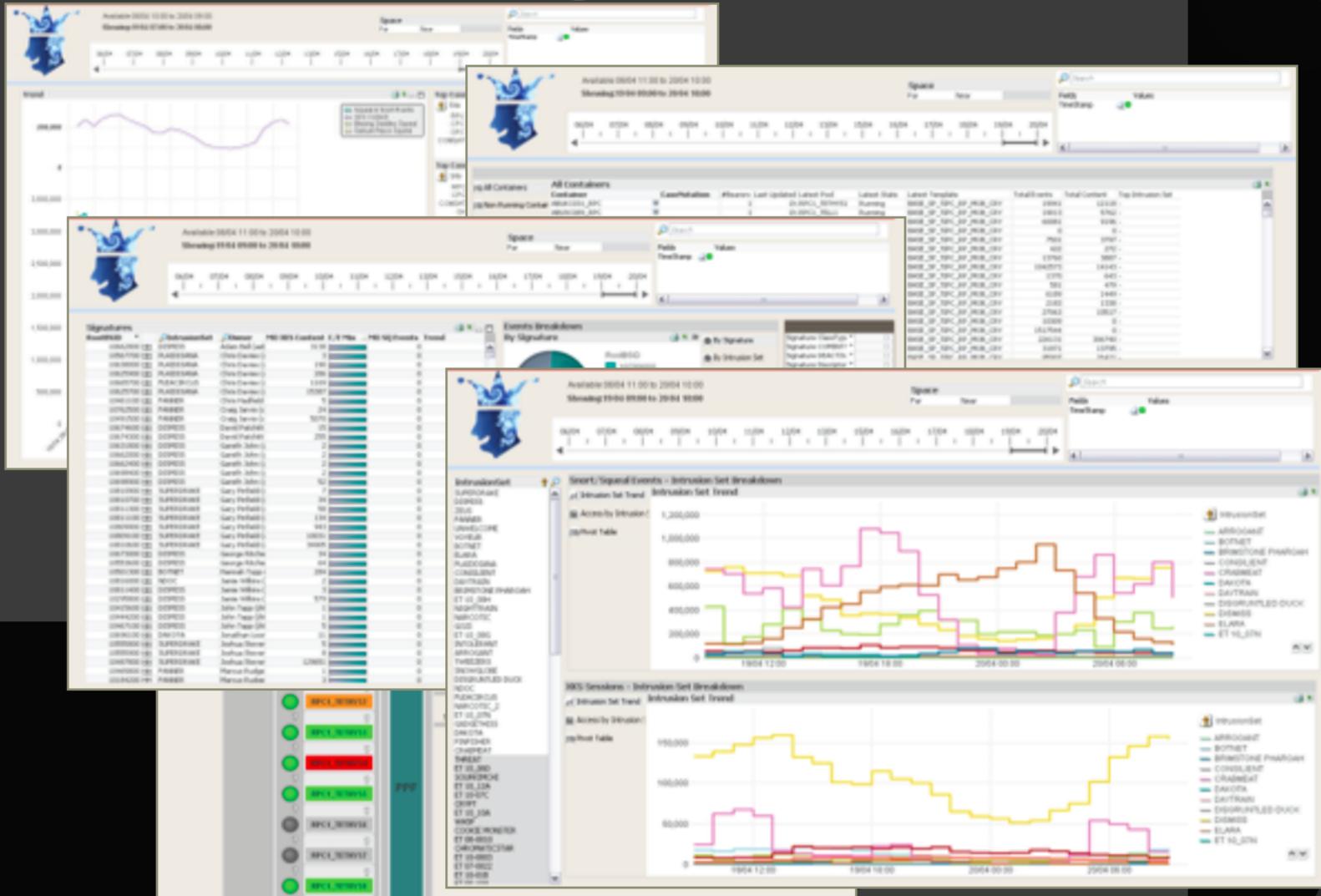


nt

Events

Knowledge

Status Checking – Fractal Joker



FRACTAL JOKER - Benefits

- Wide Vision – Sigint (TM, PPF, Blackhole, and XKS statistics) and IA Sources (GORDIAN KNOT and SPAY)
- Simple to use – Everything in it is a statistic!
- First of its kind – Simplifying PTC-world and enabling analysts understanding.

nt

Events

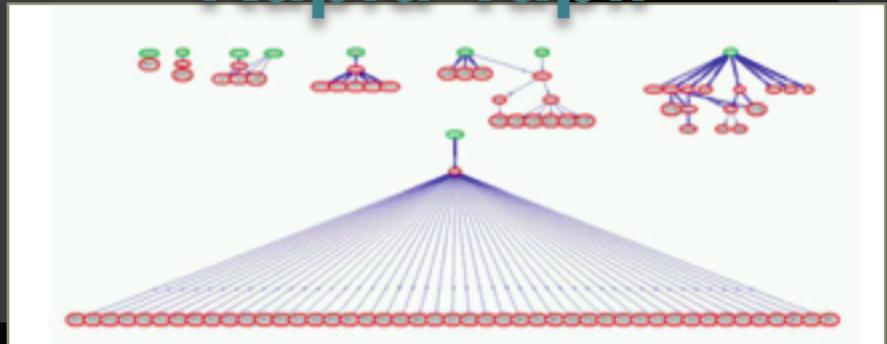
Knowl
edge

Discovery Prototypes



Crouching Squirrel

Rapid Tapir



Hidden Otter Salty Otter 8Ball in Sorcerer

nt

Events

Know
edge

Near Space Uplift.

Signature Storage

Halter Hitch

MVR/PPF

GORDIAN KNOT

SPAY

XKS

SAMUEL PEPYS

ALPINE BUTTERFLY

Gordian Knot

- ◎ More
 - 6 Full Take, GSI Logs, Local Input Sensors, and SPAY
- ◎ Faster
 - Improvements to 8Ball/PACMAN + Snort.
 - Database improvements for Analysis.
- ◎ Safer
 - Better Visualisation, Links to XKS.
- ◎ Better
 - Accredited. PKI'd. Linked to FRACTAL JOKER

Far Mid

SPAY

◎ Defence Contractors.

- After OP WAFTER
- Local 'Near' sensors to be deployed.
- Locations at UNCLASSIFIED.

Cyberwar declared as China hunts
for the West's intelligence secrets



Far Mid

IA XKS

- ◎ GORDIAN KNOT + SPAY into XKS.
- ◎ Different Legal Framework.
- ◎ Standard Search + Plugins.

Gateways

- Open Source -> Crimson
- Crimson -> GCNET
- GCNET -> Crimson
- Open Source ->GCNET (SHORTFALL)

Knowledge Base Hunt

- ◎ Challenge of finding a Cyber TKB.
 - What are we after?
 - What is out there?
 - Can we do it quickly?
- ◎ Some basic requirements existed.
 - Can I add a bit of knowledge?
 - Do I know where it came from?
 - Can I represent it? And then analyse it?

nt

Events

Knowl
edge

Knowledge Base Hunt

- TCP conducted a review of 14 different systems that might work.
- We visited 5 and tested offsite. We did the same test against BroadOak too.



nt

Events

Knowl
edge

Results.

- We learnt that there is no such thing as a TKB on the market (inside and outside).
- We then decided to try something new.



nt

Events

Knowl
edge

So WHO are Palantir?

- Palantir was comes from the team that made PayPal and was supported by In-Q-Tel (CIA Financial Wing)
- Palantir was built through iterative collaboration between Palantir computer scientists and analysts from various intelligence agencies over the course of nearly three years, through pilots facilitated by In-Q-Tel
- Palantir allows human analysts to quickly explore data from many sources in conceptual ways

nt

Events

Knowl
edge

Normal Analyst Workflow



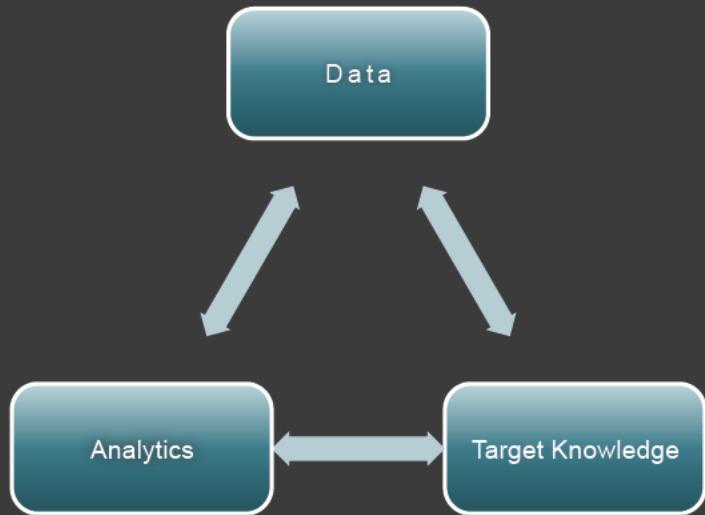
This is our usual model. Access gets us Data. We do Analytics on that Data. Target Knowledge is the result. Each is done in it's own tool, not brought together.

nt

Events

Knowl
edge

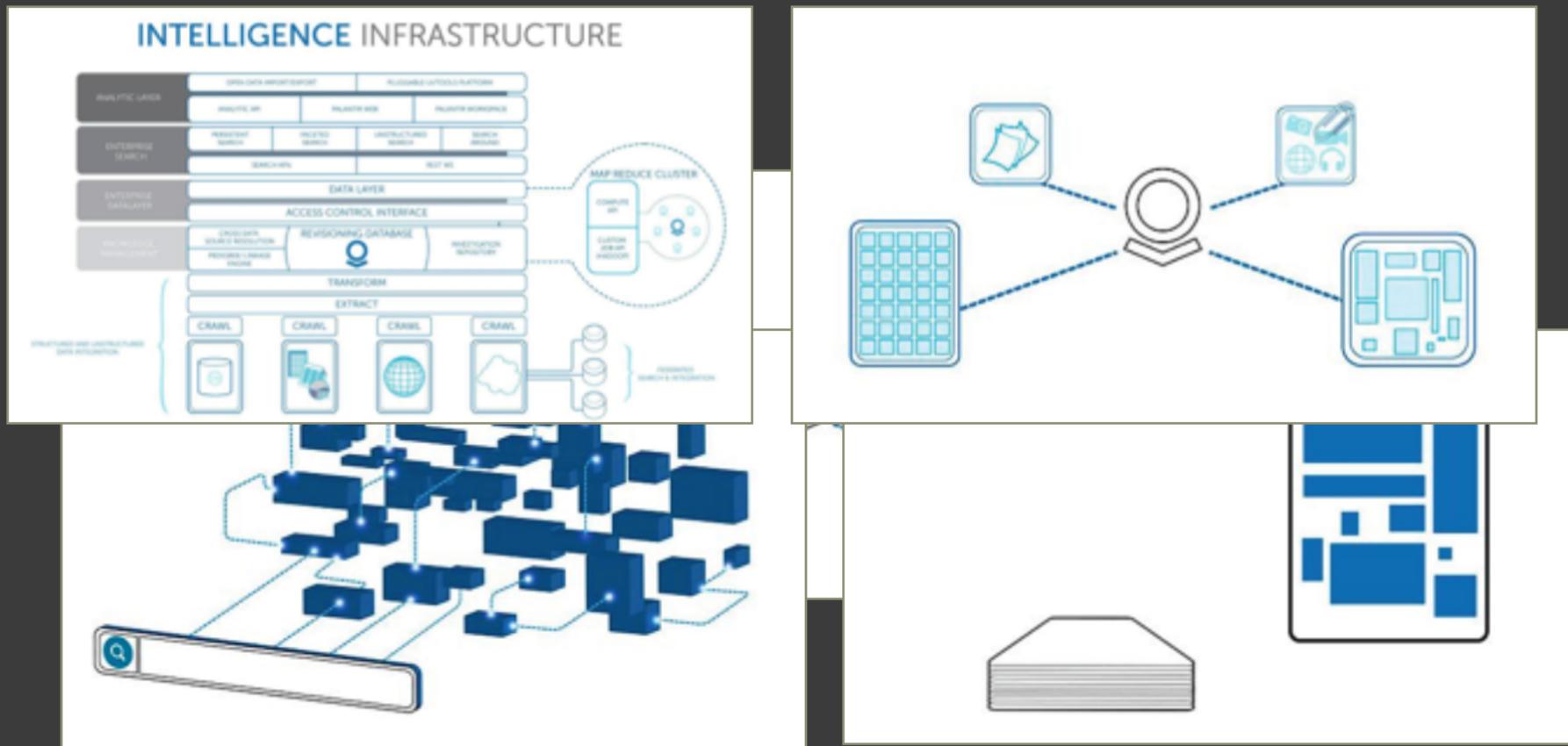
Why is Palantir different?



This is the Palantir Model.

Data can come from anywhere, asked whatever the analyst wants, and it will enrich from the sum of the Target Knowledge – Palantir itself.

So WHAT is Palantir?



4 Pillars: Collaboration, Knowledge Management, Search and Discovery, Data Integration.

4 ways to get data in: Manual, Automatic, Raptor, Helper.

Does it work? You decide...

The screenshot shows the XKEYSCORE (LIVE) interface. On the left, there are several buttons: 'Add to graph', 'Refresh query list', 'Choose new node colour (First)', 'Choose new node colour (Last)', and 'Auto-merge links'. The main area displays a table with columns: 'Add to Graph', 'Query Name', and 'Status'. The data includes:

Add to Graph	Query Name	Status
	WalkerGold_Marcus	finished
	NTCom_Marcus2	38
	DancingPanda_Rab	97
	Makersmark_Craig	finished
	Makersmark_Craig	finished

Below this is a large table titled 'Detailed Log' with columns: 'File ID', 'Source IP', 'Status', 'Event Date', 'Event Details', 'Event Date', and 'Event Submitter'. The table contains numerous rows of log entries.

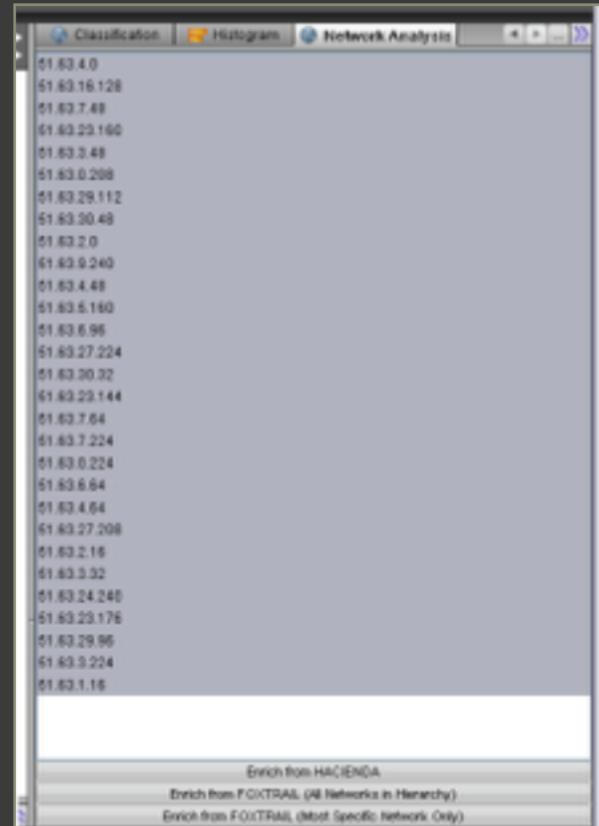
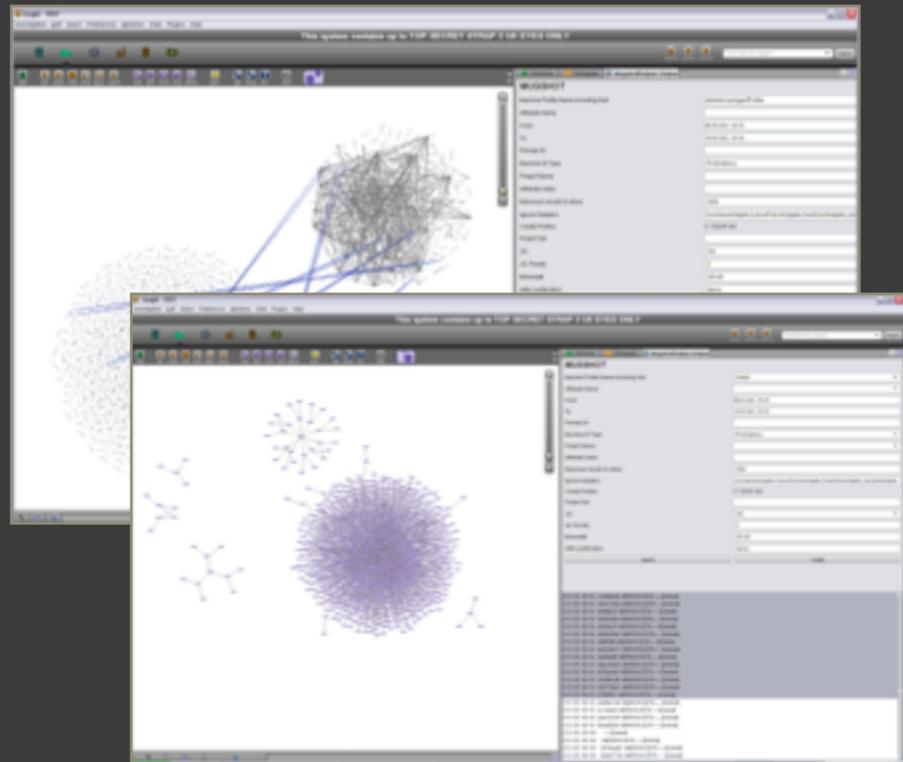
The screenshot shows the GEOFUSION interface. At the top, there are tabs: 'Selection', 'Histogram', and 'Geofusion'. The 'Geofusion' tab is selected. Below the tabs are fields for 'IP', 'Domain', 'Geo', 'City', 'Country', 'Company', and 'Nationality'. There are also 'Update', 'Select All', and 'Select None' buttons. A vertical slider is on the left. The main area lists IP addresses with their enrichment details:

- 51.63.30.128 (Unknown - UK Government Department for Work and Pensions)
- 51.63.3.80 (Unknown - UK Government Department for Work and Pensions)
- 51.63.9.64 (Unknown - UK Government Department for Work and Pensions)
- 51.63.26.80 (Unknown - UK Government Department for Work and Pensions)
- 51.63.30.0 (Unknown - UK Government Department for Work and Pensions)
- 51.63.8.112 (Unknown - UK Government Department for Work and Pensions)
- 51.63.3.96 (Unknown - UK Government Department for Work and Pensions)
- 51.63.3.64 (Unknown - UK Government Department for Work and Pensions)
- 51.63.30.176 (Unknown - UK Government Department for Work and Pensions)
- 51.63.8.176 (Unknown - UK Government Department for Work and Pensions)
- 51.63.8.0 (Unknown - UK Government Department for Work and Pensions)
- 51.63.8.160 (Unknown - UK Government Department for Work and Pensions)
- 51.63.29.128 (Unknown - UK Government Department for Work and Pensions)
- 51.63.27.64 (Unknown - UK Government Department for Work and Pensions)
- 51.63.29.0 (Unknown - UK Government Department for Work and Pensions)
- 51.63.27.144 (Unknown - UK Government Department for Work and Pensions)
- 51.63.30.16 (Unknown - UK Government Department for Work and Pensions)
- 51.63.30.160 (Unknown - UK Government Department for Work and Pensions)

**Direct XKS Results + Click
to Content.**

**GEOFUSION Automatic
Enrichment.**

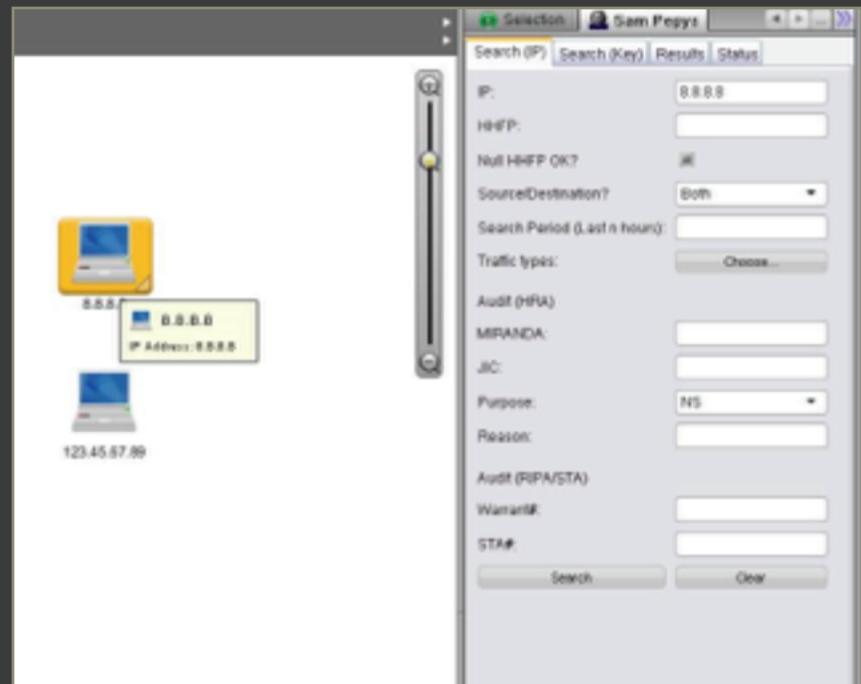
And...



MUGSHOT Integration

HACIENDA / FOXTRAIL enrichment

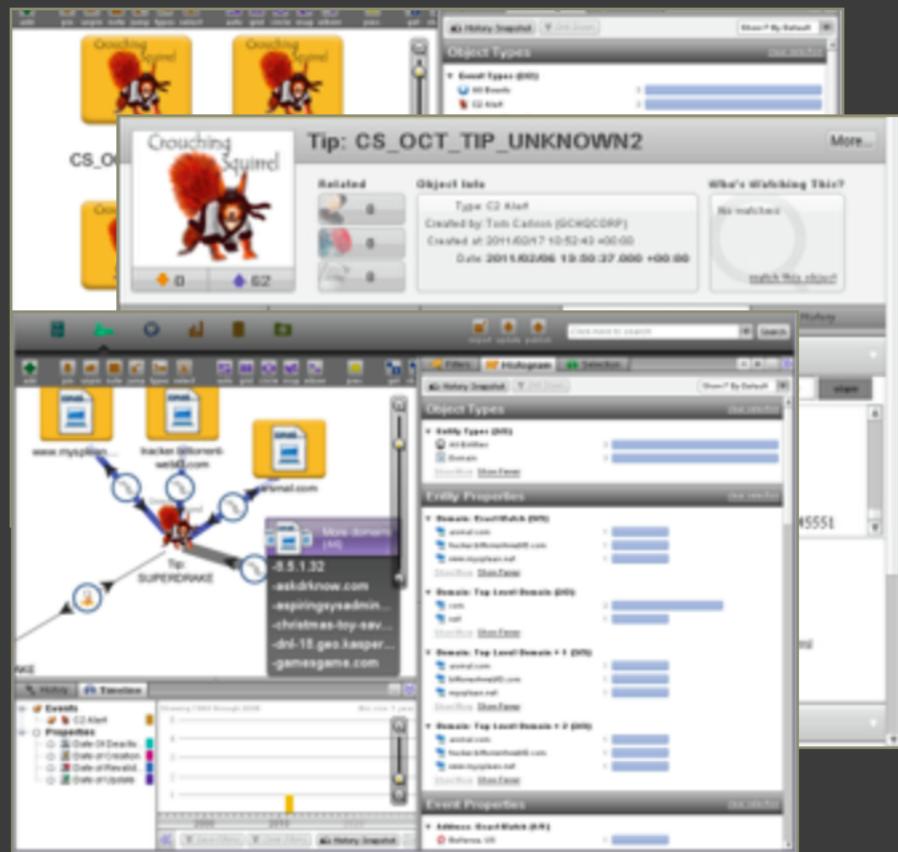
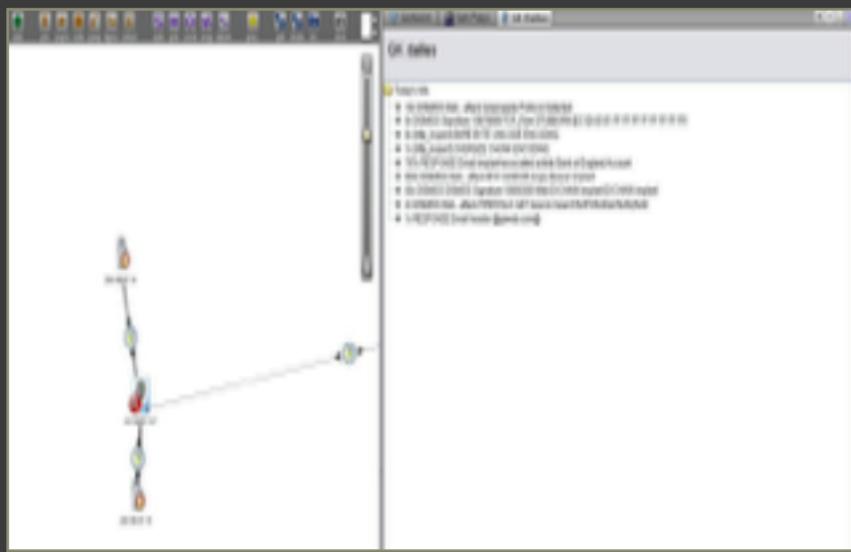
And....



Google Earth Representation

SAMUEL PEPYS Events generation

And.....



GORDIAN KNOT integration: Snort and 8BALL

RAPID TAPIR/ CROUCHING SQUIRREL – New Prototypes!

nt

Events

Knowl
edge

Palantir - Benefits.

- Faster Analytics.- Ecrime team can find C&C ORBs faster, just by ingesting files.
- Target Knowledge Storage – Fanner have already run OP DEVICE on it. The sharing of ‘knowledge’ got results.
- Easy Development – Already 3 helpers not steered by NDIST. MUGSHOT/ GLOBAL SURGE/RAPID TAPIR.

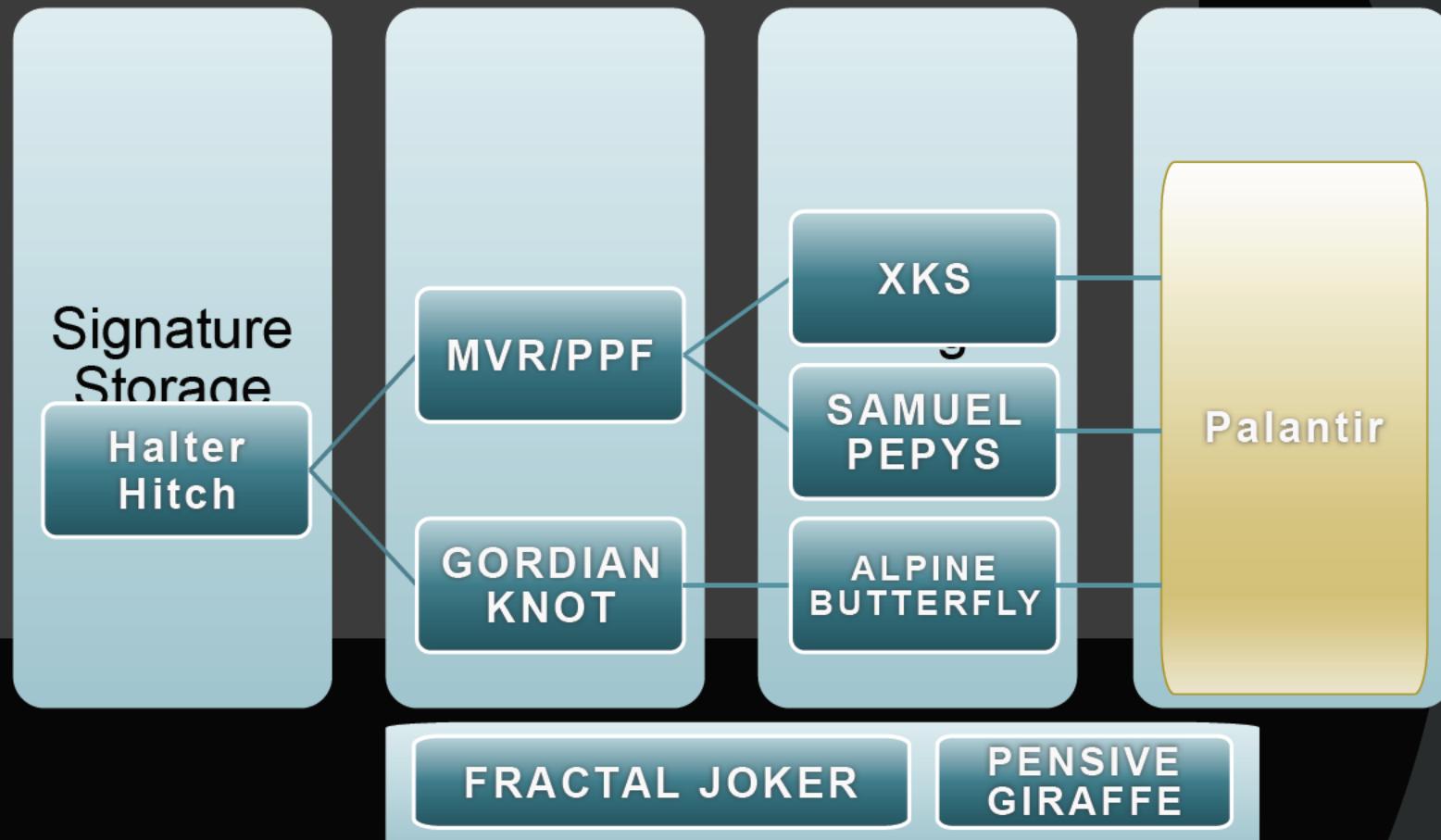
nt

Events

Knowl
edge

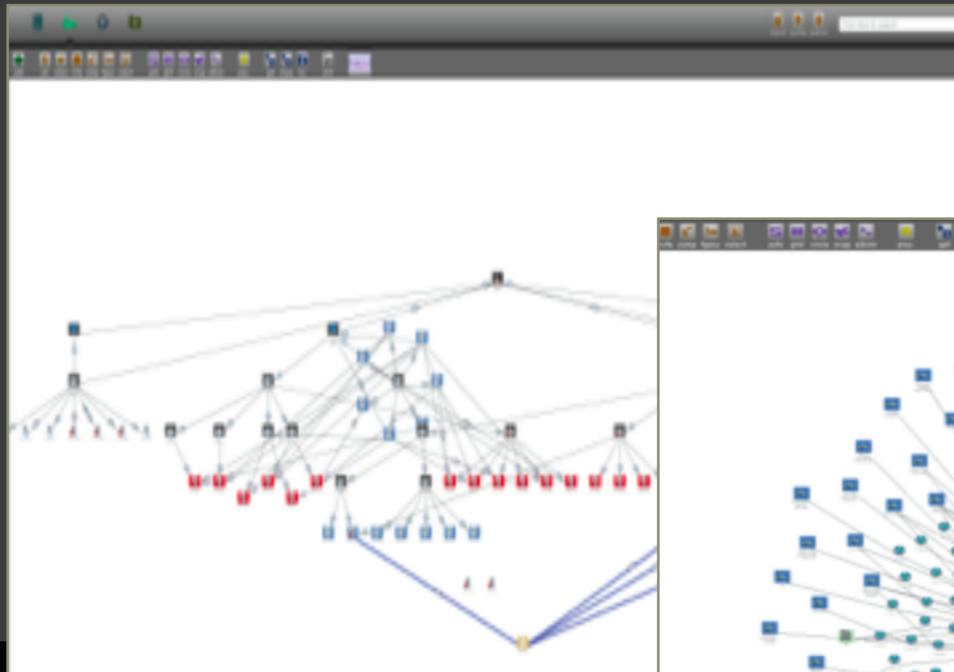
Comments from Analysts:

Where does it sit?

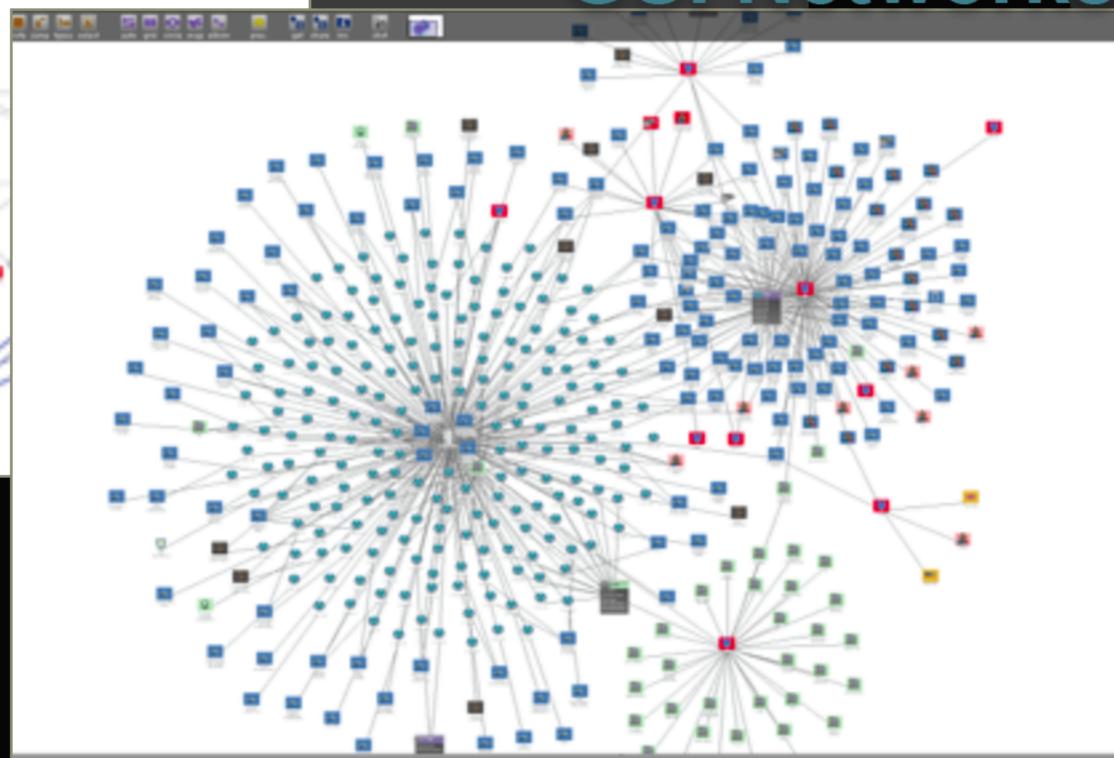


++Navigation, Fusion, Investigation Mgmt and Presentation

Here is existing Target Knowledge



Fanner Groups



GSI Networks

nt

Events

Knowl
edge

The Goal.

- End to End tracing.
From Warrant to Signature; Signature to Events/Content; to End Product or CNE!
- But also do the reverse! From Vulnerability to Malware, from Malware to Actor, from Actor to Modus Operandi.

Status

nt

Events

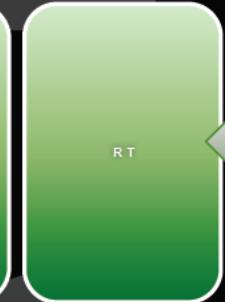
Knowl
edge

Palantir

Workspace



Events



Enrichment

nt

Events

Knowl
edge

Unexpected Benefits

- Nexus Peering – We can link our Palantir, to the DSD version, or maybe Special Forces?
- Interacts with anything! – DISTILLERY, Hadoop, QFD's, Google Earth (Incl. DSLive!)
- Security Model is core to the system
- Exploit system, enabling Prototypes!
- Legal Audit/Training/CapDev is easier
- You can even use it on a iphone or laptop

nt

Events

Knowl
edge

Potential Downsides

- Looks Expensive! Well not really. That depends on your Data size, not users. Development Servers are free. Live isn't as expensive as expected
- Is it scalable? Well seems to work for us, FBI+DSD have much bigger implementations.
- What can't it do? Well it isn't perfect! However we ask, Palantir answer.

nt

Events

Knowl
edge

What is next?

Far

Standard Targeting/Testing system – Evolved Targeting.

Cloud Analytics.

Discovery / Behavioural Analysis

Mid

Active Defence options

Data Acquisition (Open Source?).

Near

More SPAY deployments

Optimising of GK – More advanced heuristics.

Questions?

er

Techn
ology

Victim

-
-