

[REDACTED] – 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 10<sup>th</sup> 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



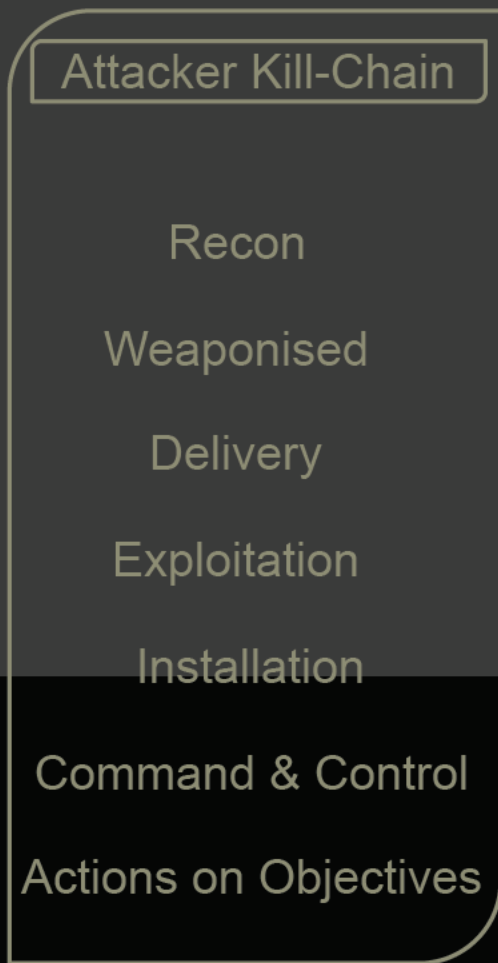
Modus Operandi  
Tracking/Discovery



Maturity

Threat Tracking

# The Asymmetric Challenge

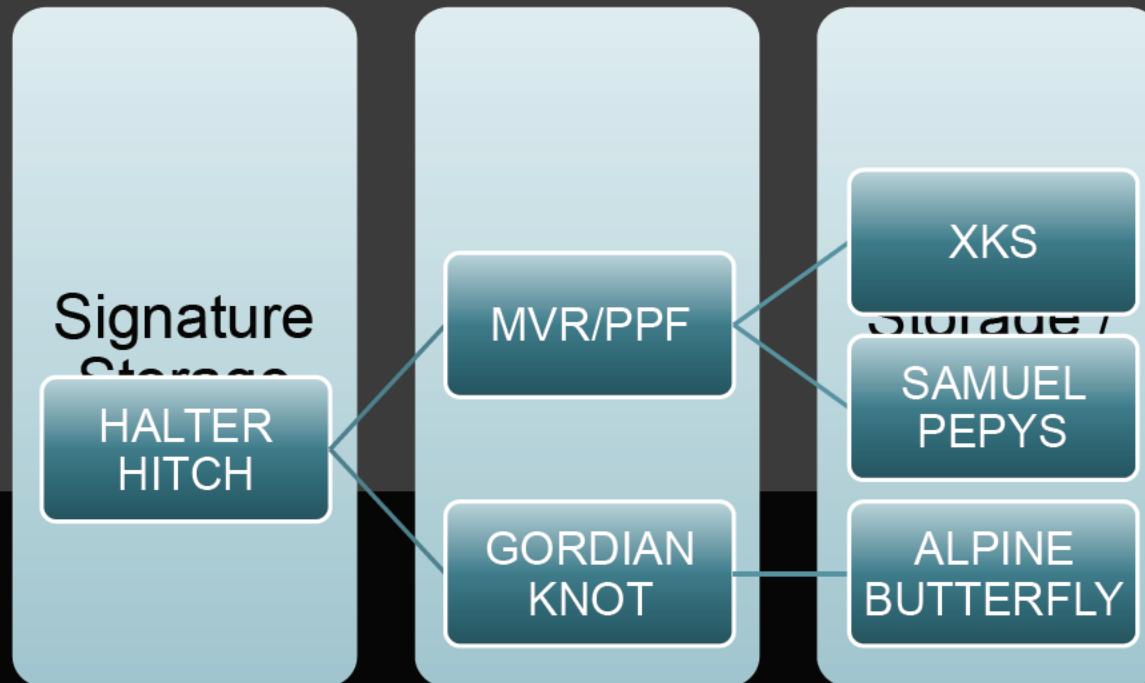


# May 2010

Far

Mid

At the turn of the new Financial Year we had:





# Sigint Story

Far

Mid

- ◉ Started at 13 x 10g Bearers
- ◉ Presently at 180 x10g Bearers
- ◉ From 1000 Signatures
- ◉ To 2500 Signatures
- ◉ Including Tryst and Comsat





# Challenges ahead

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

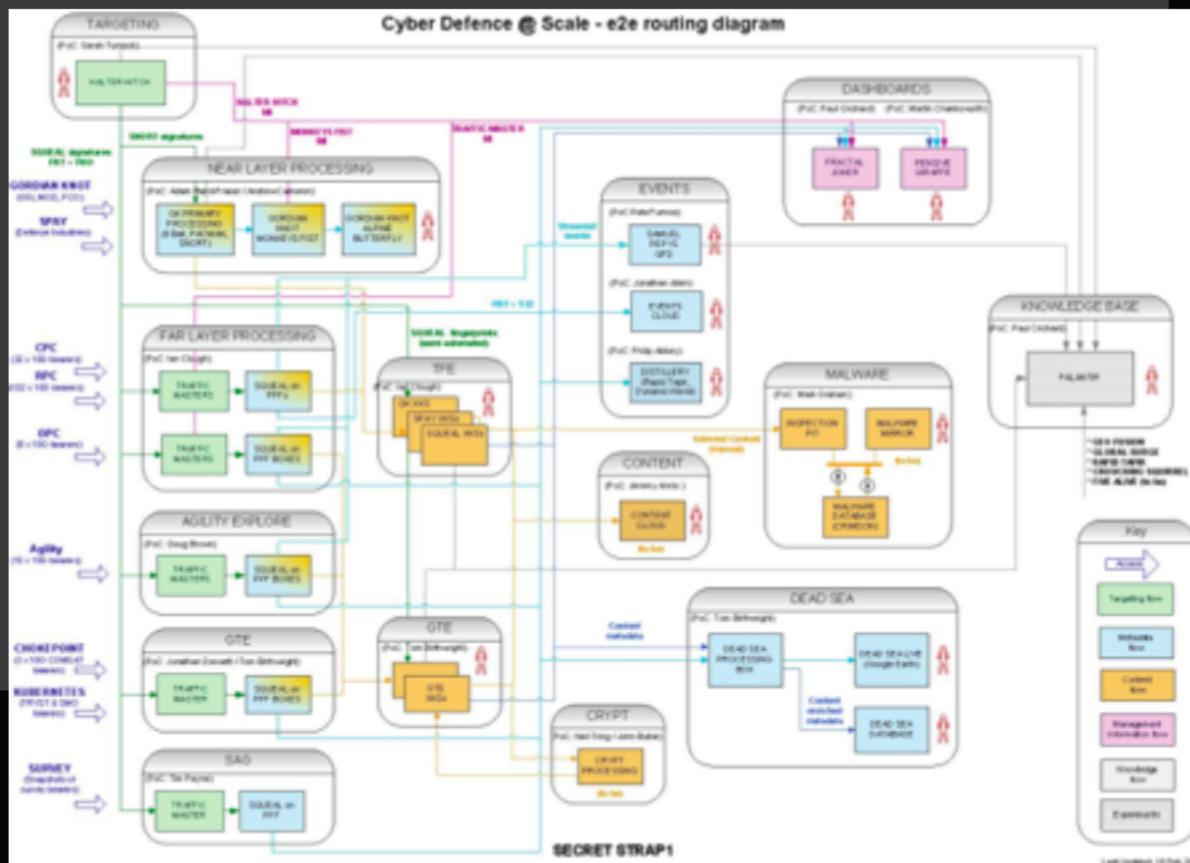
nt  
Events Knowledge

nt

# What about the Sigint Collection?

Events

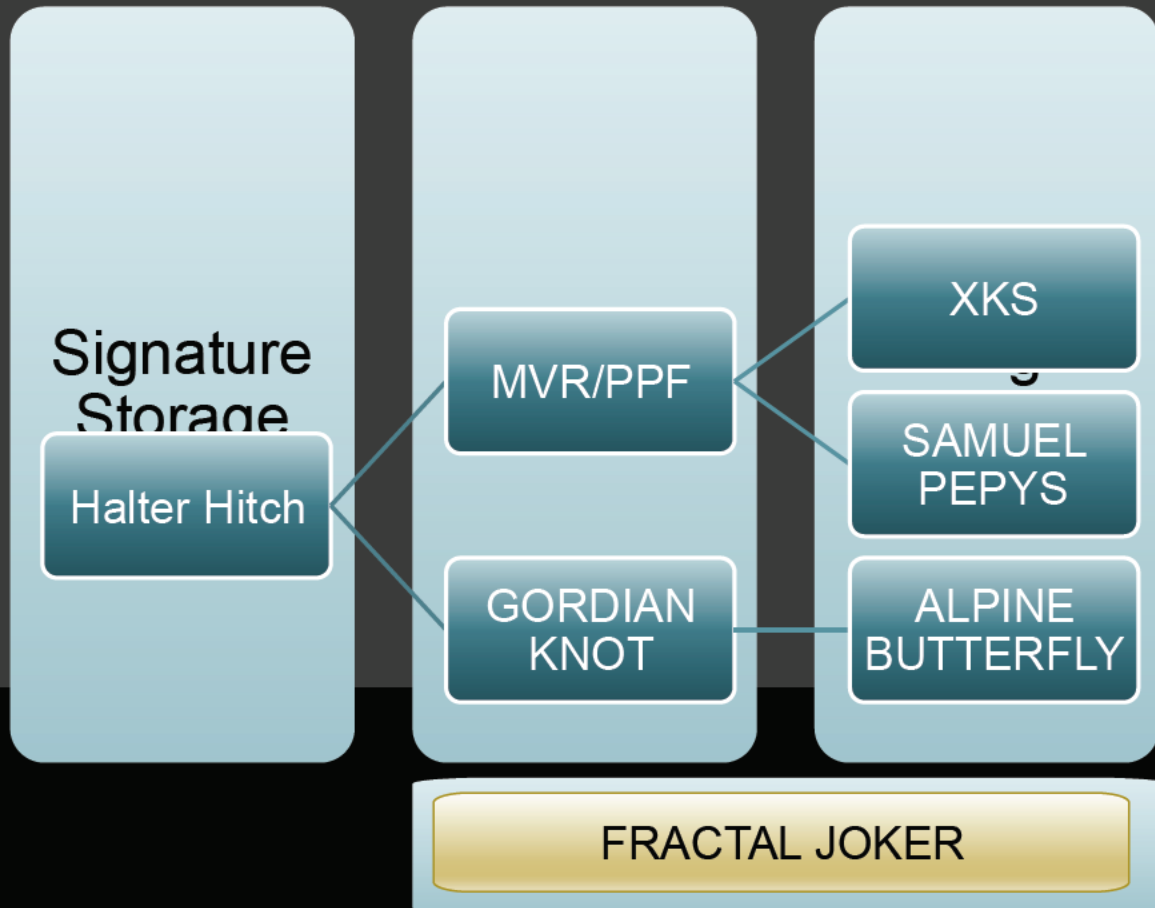
Knowl  
edge



# What is the state of collection?

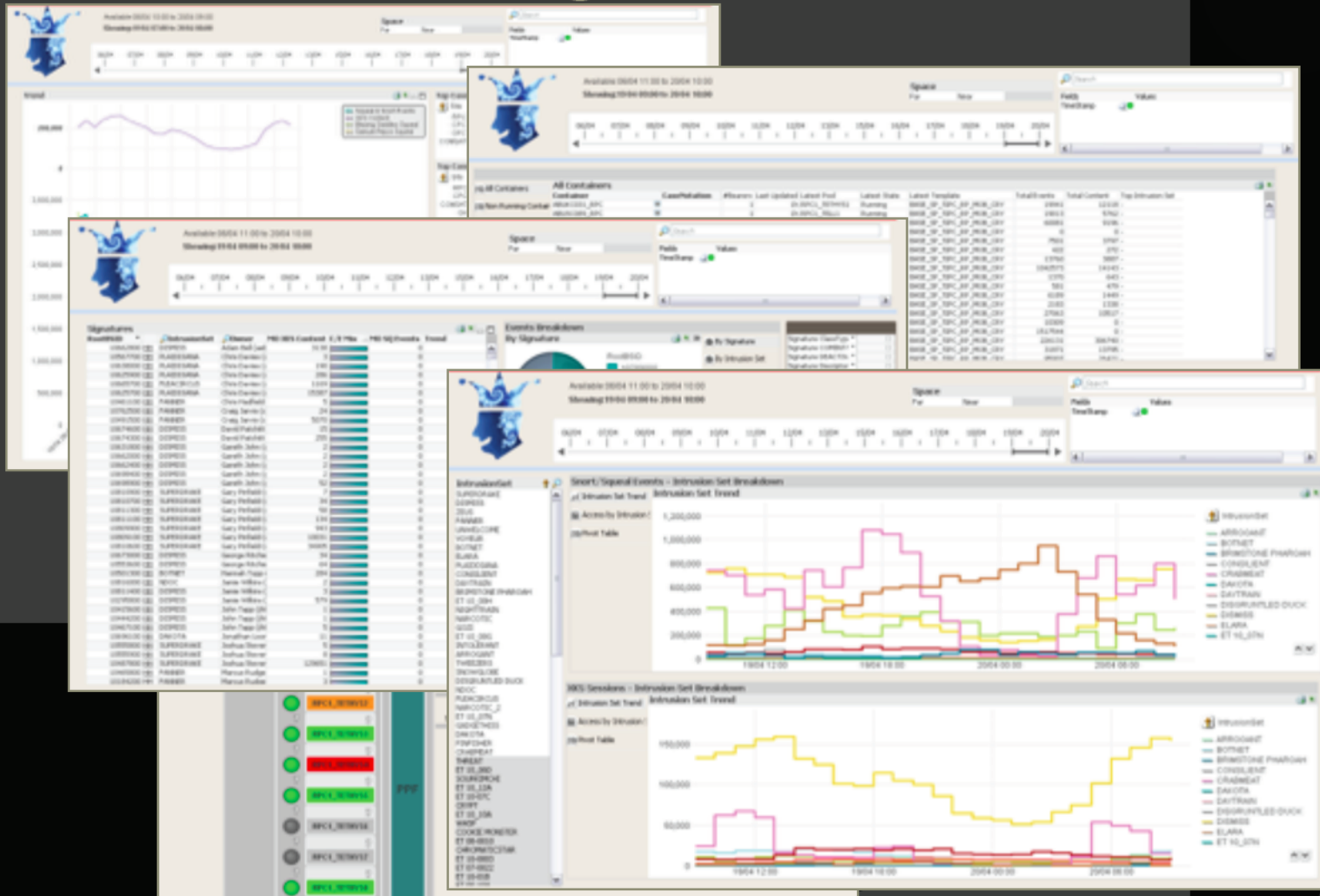
Events

Knowl  
edge



# Status Checking – Fractal Joker

nt  
Events  
Knowl  
edge



# FRACTAL JOKER - Benefits

nt

Events

Knowl  
edge

- ◉ 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 it's kind – Simplifying PTC-world and enabling analysts understanding.



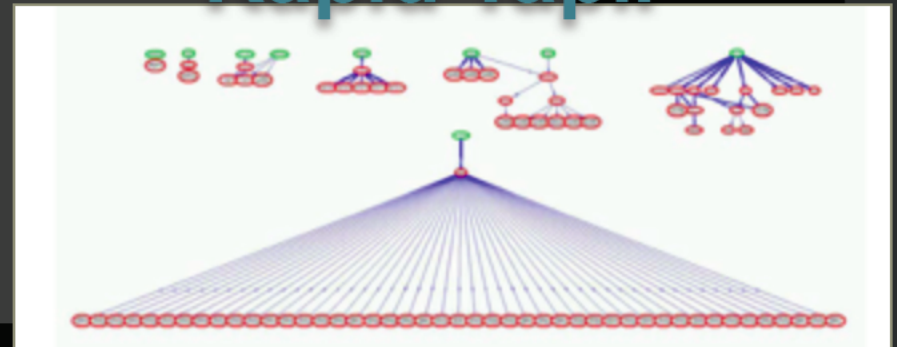
# Discovery Prototypes

nt  
Events Knowledge



Crouching Squirrel

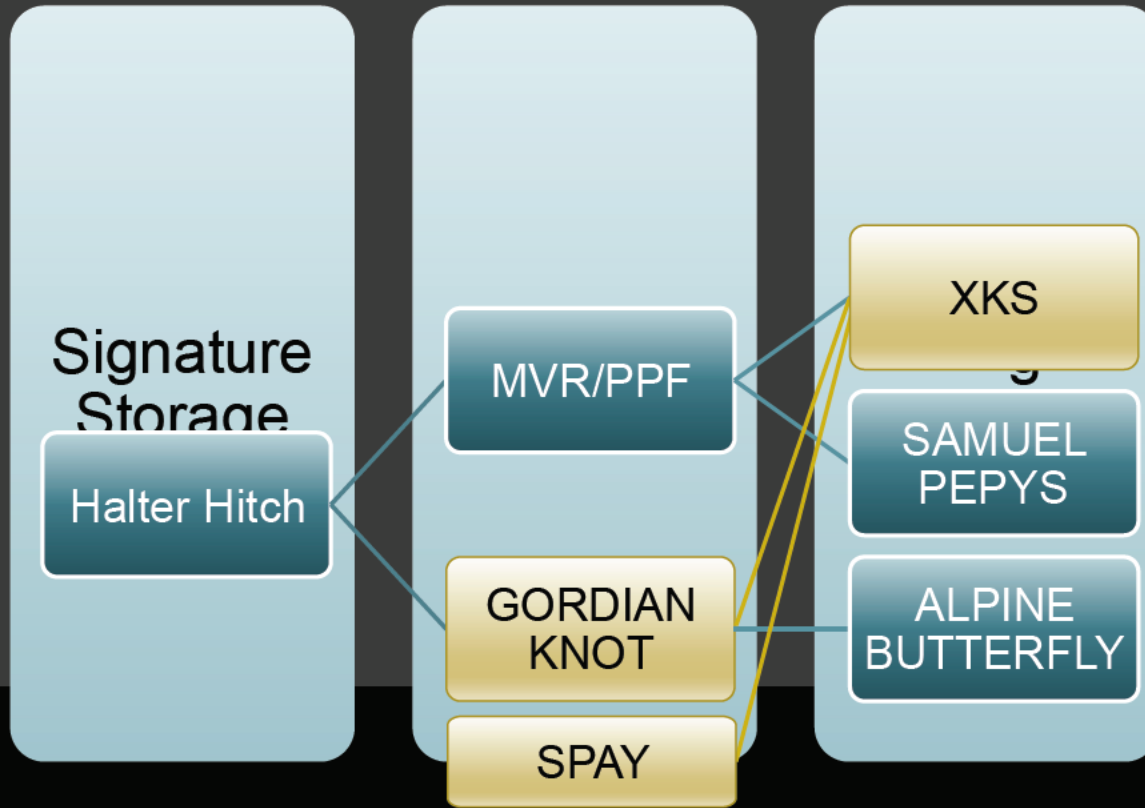
## Rapid Tapir



Hidden Otter  
Salty Otter  
8Ball in Sorcerer

# Near Space Uplift.

nt  
Events Knowledge





# Gordian Knot

Far Mid

- ◉ 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

# SPAY

Far Mid

- ◎ 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**



# IA XKS

Far Mid

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

# Gateways

Far

Mid

- ◉ 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 Knowledge

# 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 Knowledge

# 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 Knowledge



# 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 Knowledge

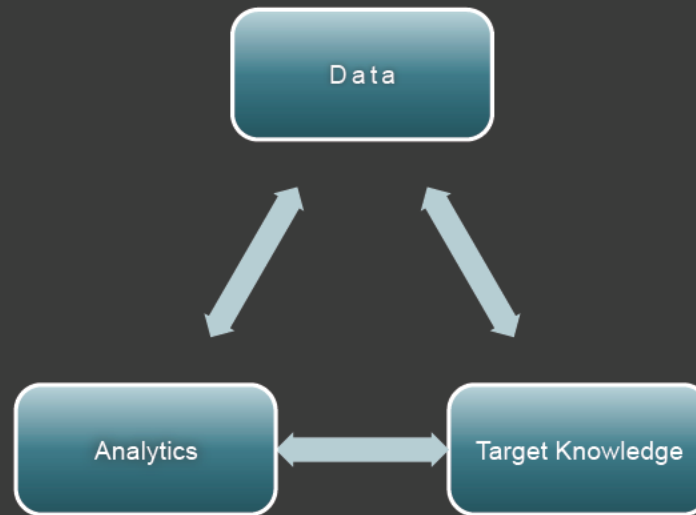
# Normal Analyst Workflow



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 Knowledge

# Why is Palantir different?

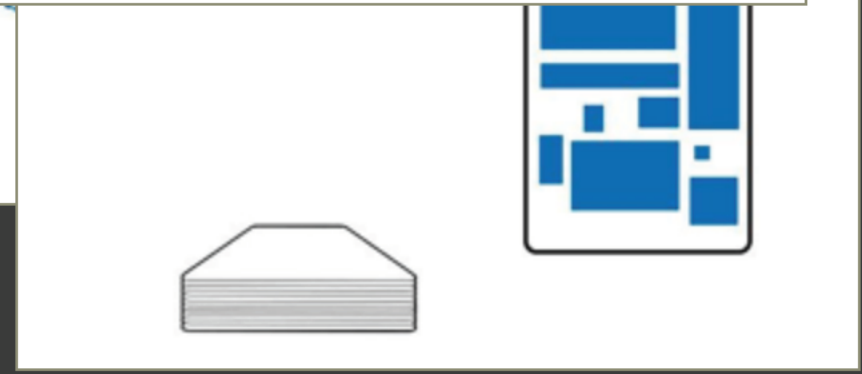
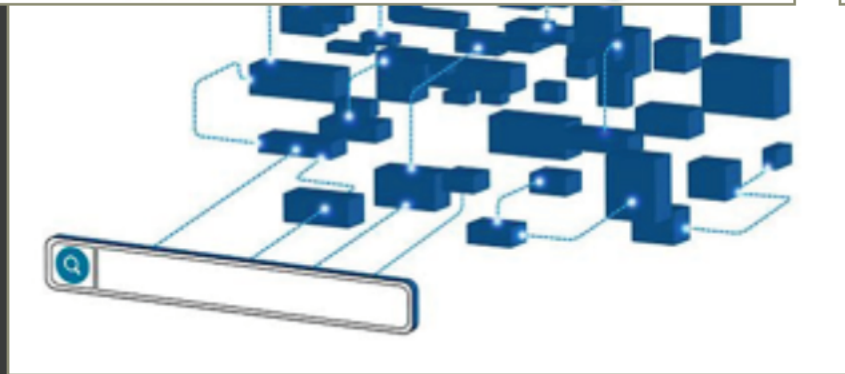
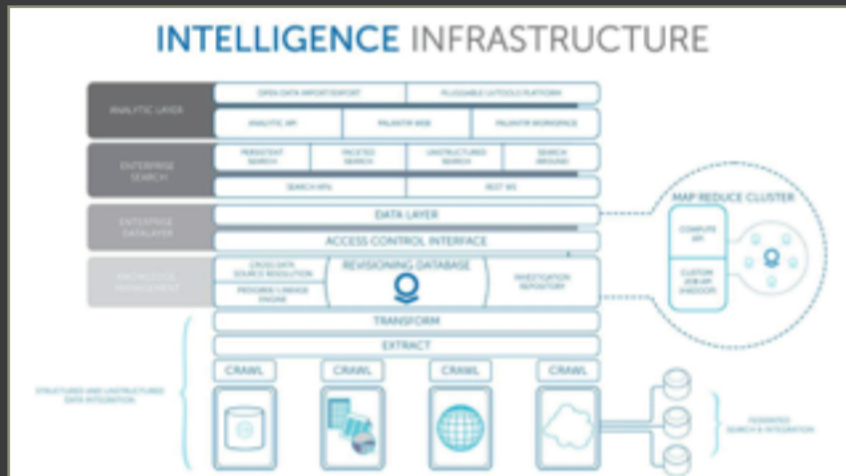


This is the **Palantir Model**.

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

nt  
Events Knowledge

# 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...

XKEYSCORE (LIVE)

Add to graph

Refresh query list

Choose new node colour (First)

Choose new node colour (Last)

Auto-merge links

Add to Graph	Query Name	Status
<input type="checkbox"/>	WalkerGold_Marcus	finished
<input type="checkbox"/>	NTCom_Marcus2	98
<input type="checkbox"/>	DancingPanda_Rob	97
<input type="checkbox"/>	Makersmark_Craig	finished
<input type="checkbox"/>	Makersmark_Craig	finished

Auto-merge links

IP	Domain	Geo	City	Country	Company	Nationality
51.63.30.128	Unknown	UK				
51.63.30.80	Unknown	UK				
51.63.9.64	Unknown	UK				
51.63.26.80	Unknown	UK				
51.63.30.0	Unknown	UK				
51.63.8.112	Unknown	UK				
51.63.9.96	Unknown	UK				
51.63.3.64	Unknown	UK				
51.63.30.176	Unknown	UK				
51.63.8.176	Unknown	UK				
51.63.8.0	Unknown	UK				
51.63.8.160	Unknown	UK				
51.63.29.128	Unknown	UK				
51.63.27.64	Unknown	UK				
51.63.29.0	Unknown	UK				
51.63.27.144	Unknown	UK				
51.63.30.16	Unknown	UK				
51.63.30.160	Unknown	UK				

Selection Histogram Geofusion

Single IP Selected

IP: 51.63.30.128

Domain: Unknown

Geo: UK

City:

Country: UK

Company:

Nationality:

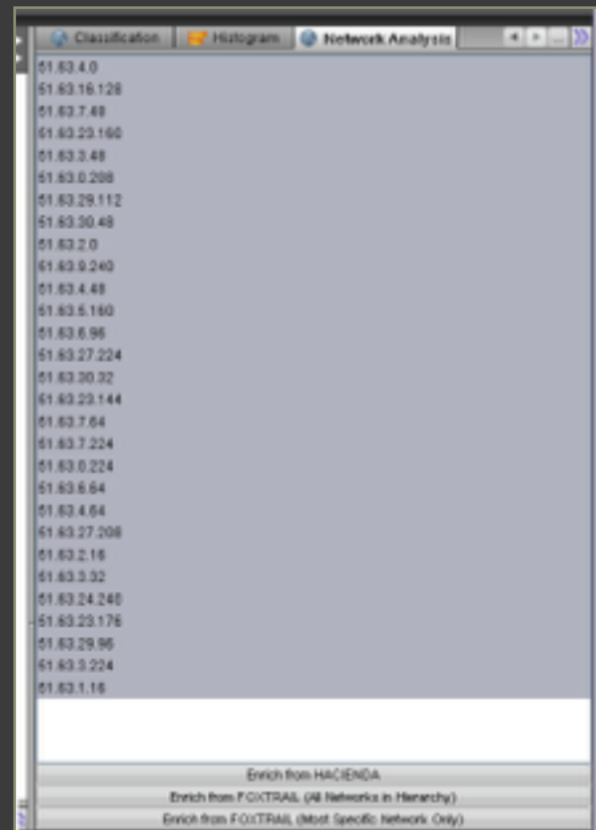
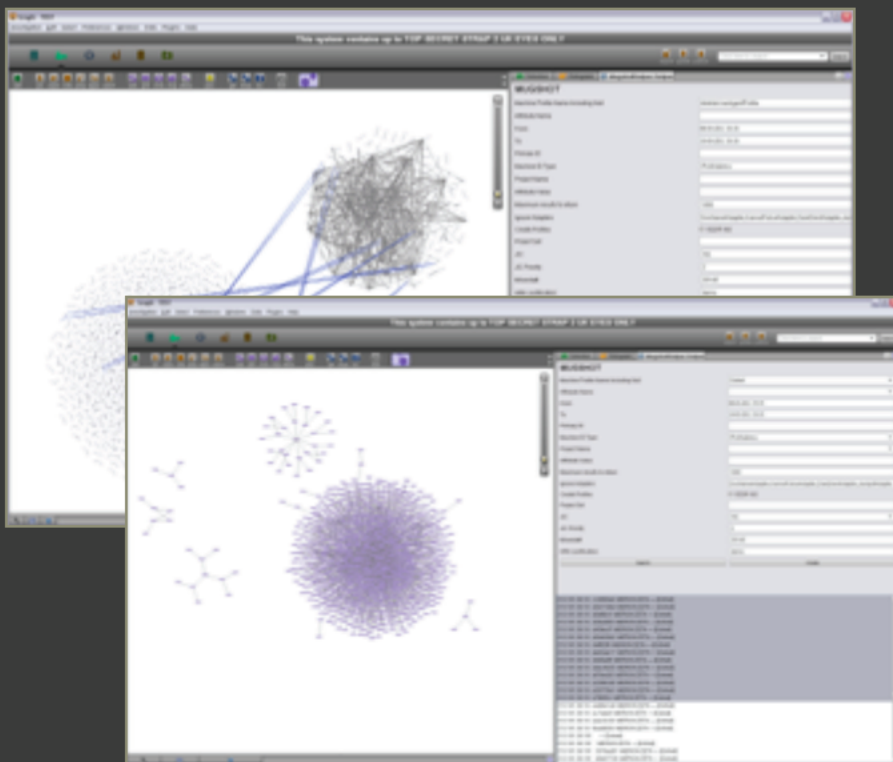
Update Select All Select None

- 51.63.30.128 (Unknown - UK Government Department for Work and Pensions)
- 51.63.30.80 (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)
- 51.63.9.96 (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.

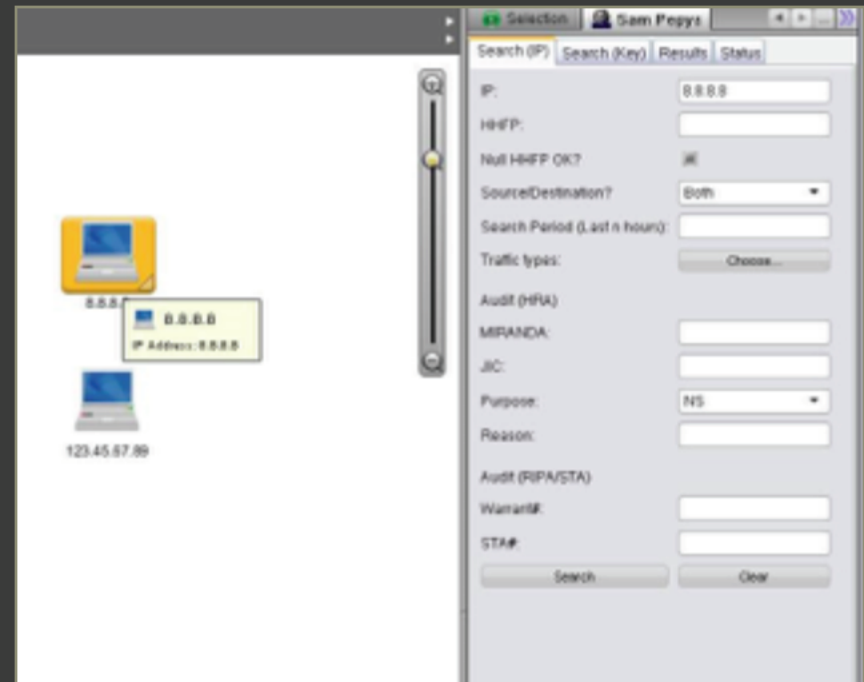
# And...



## MUGSHOT Integration

## HACIENDA / FOXTRAIL enrichment

# And....

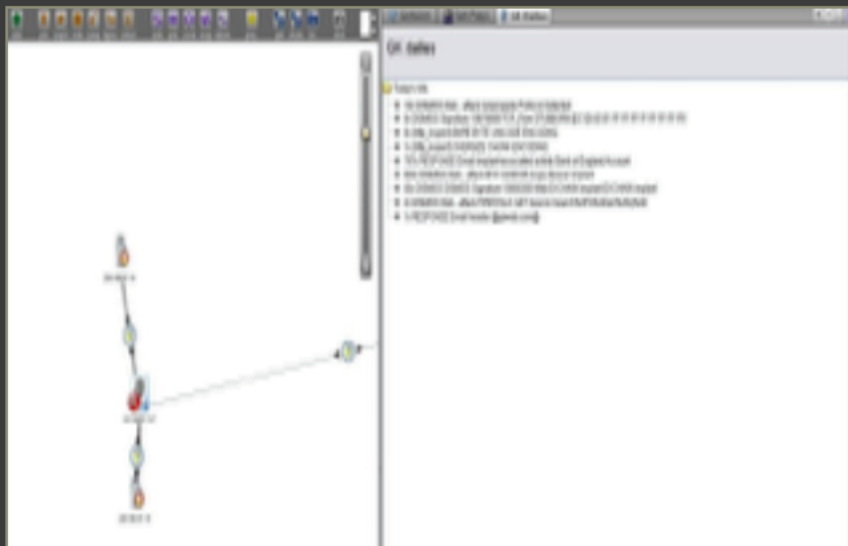


## Google Earth Representation

## SAMUEL PEPYS Events generation



And.....



A screenshot of a security information and event management (SIEM) interface. The main window displays a network diagram with nodes and connections. A pop-up window titled "Tip: CS\_OCT\_TIP\_UNKNOWN2" is overlaid on the diagram. The tip window shows a "Crouching Squirrel" icon and details for a "Type: CS Alert". Below the tip window, a list of related events is visible, including "Tip: SUPEROWIE" and "ask2know.com". The interface also shows a "History" pane on the right with a list of events and their properties.

**GORDIAN KNOT** integration:  
Snort and 8BALL

**RAPID TAPIR/ CROUCHING  
SQUIRREL** – New Prototypes!

# Palantir - Benefits.

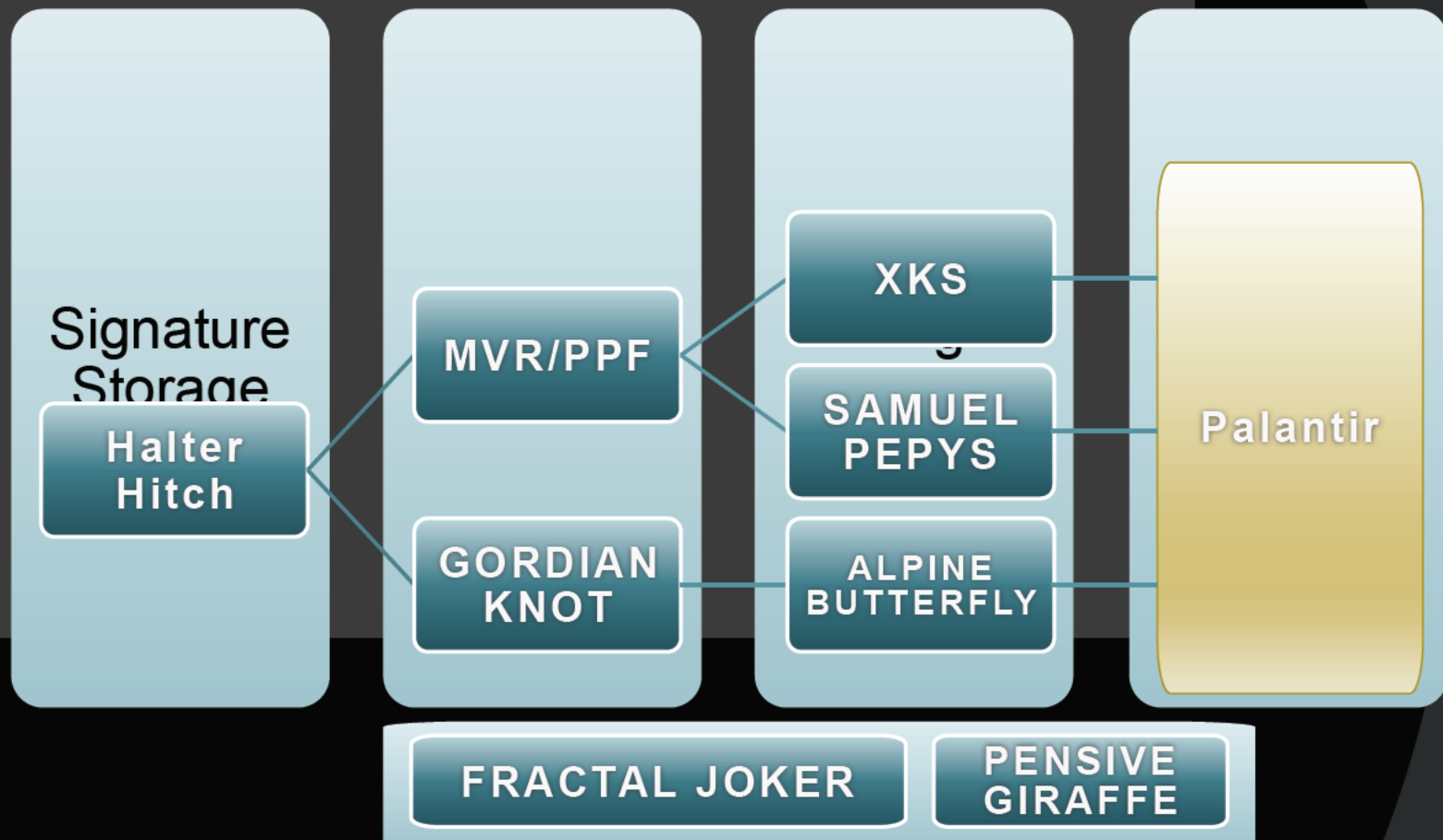
- ◉ Faster Analytics.- **Ecrime** team can find C&C ORBs faster, just by ingesting files.
- ◉ Target Knowledge Storage – **Fanner** have already run **OP DEVICE** on it. The sharing of ‘knowledge’ got results.
- ◉ Easy Development – Already 3 helpers not steered by **NDIST. MUGSHOT/ GLOBAL SURGE/RAPID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

nt  
Events Knowledge

# Comments from Analysts:

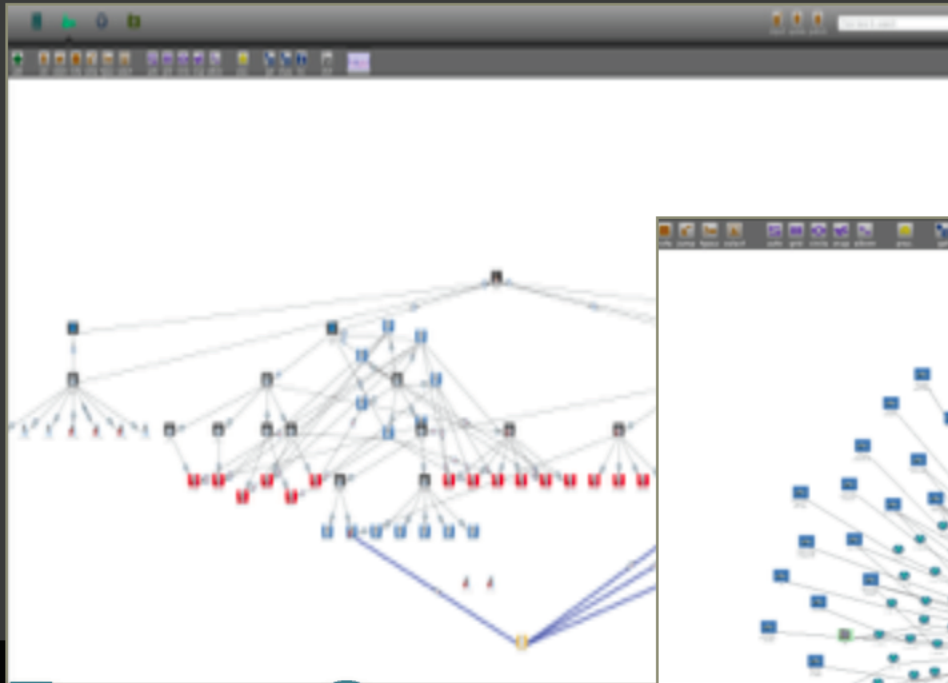


# Where does it sit?



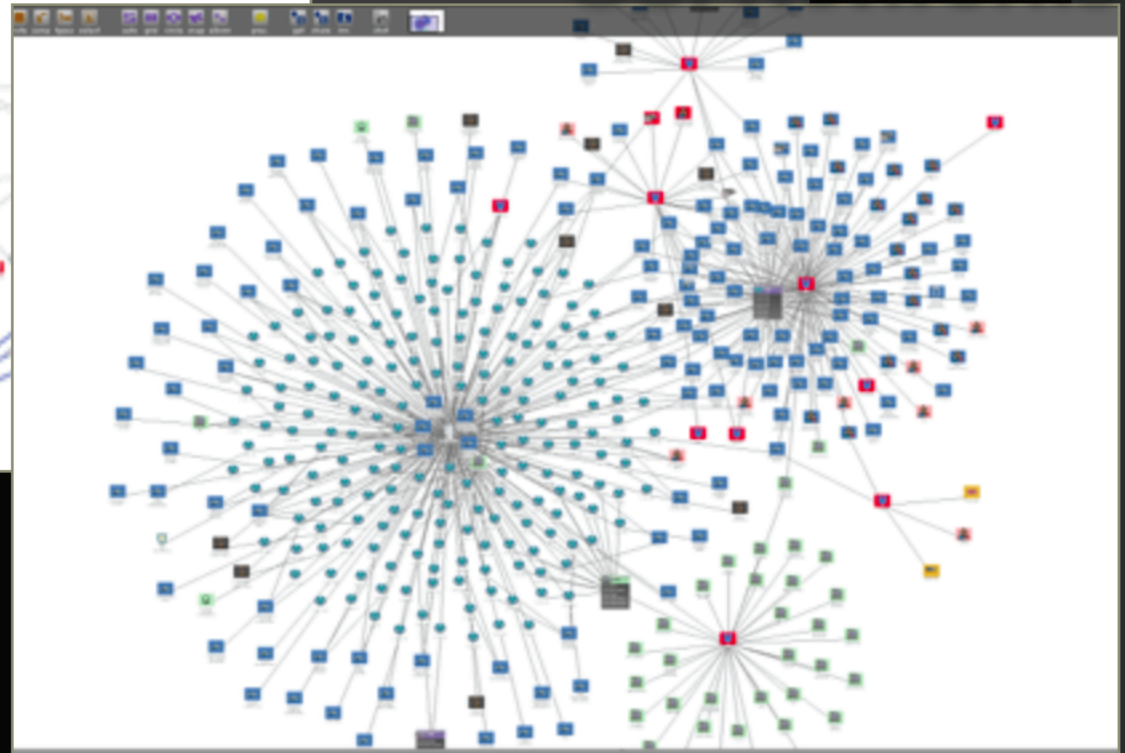
++Navigation, Fusion, Investigation Mgmt and Presentation

# Here is existing Target Knowledge



Fanner Groups

## GSI Networks



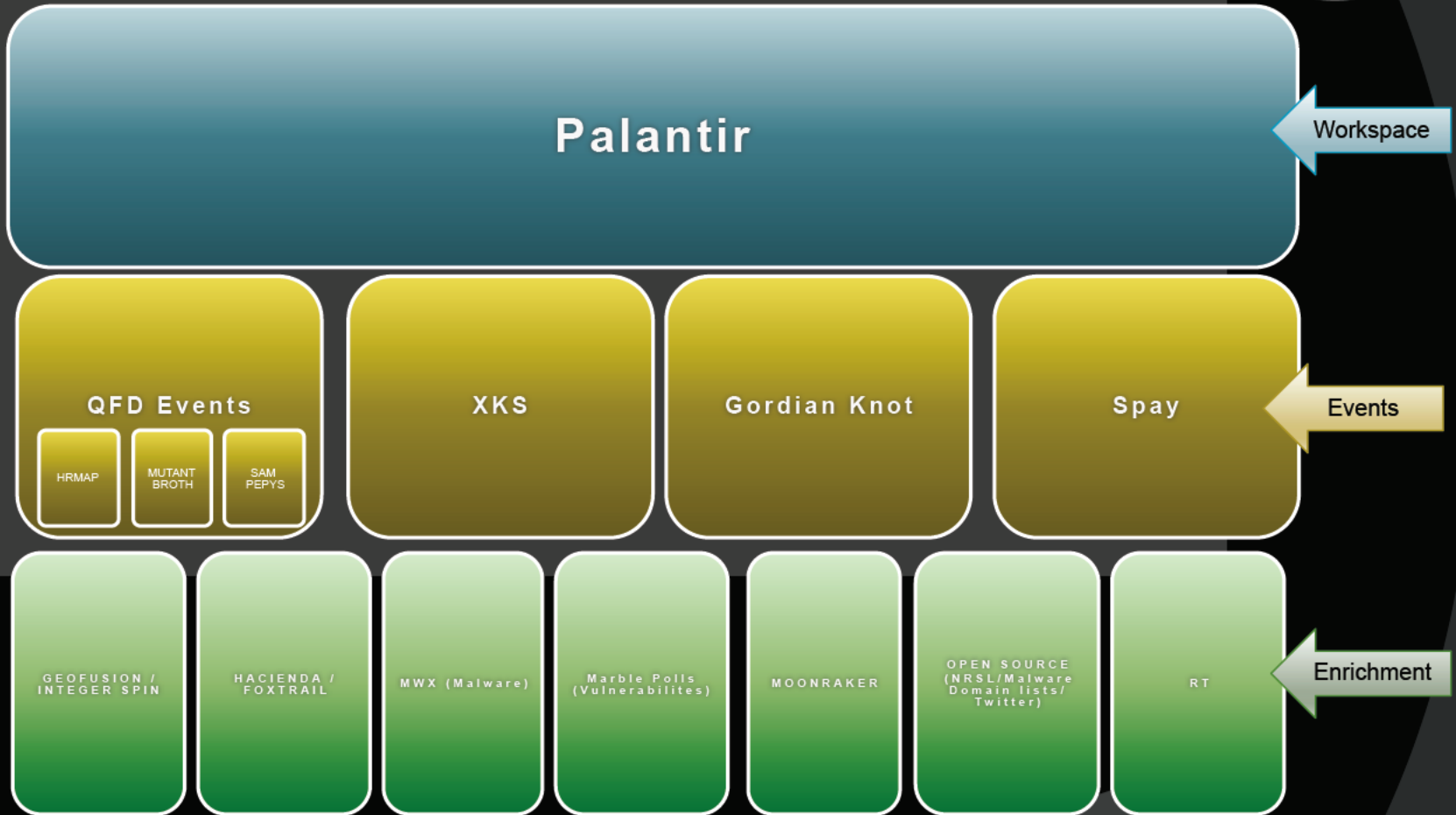
# The Goal.

- ◉ 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.

nt  
Events Knowledge

# Status

nt  
Events Knowledge



# 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 Knowledge



# 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 Knowledge

# What is next?

nt  
Events Knowledge

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



[Redacted]



[Redacted]

