



**AND THEY SAID TO THE  
TITANS: « WATCH OUT  
OLYMPIANS IN THE  
HOUSE! »**

**CSEC – Advanced Network Tradecraft  
SD Conference June 2012**

**Overall Classification: TOP SECRET//SI**

# OLYMPIA & THE CASE STUDY



## CSEC's Network Knowledge Engine

Various data sources  
Chained enrichments  
Automated analysis

## Brazilian Ministry of Mines and Energy (MME)

New target to develop  
Limited access/target knowledge



## QUESTIONS

- How can I use the information available in SIGINT data sources to learn about the target?
- What can I find that would help me inform access development efforts?
- Can I automate the analytical process and/or reuse analytics designed for other purposes?



# OLYMPIA AT A GLANCE

The screenshot displays the Advanced Network Tradecraft (ANT) software interface, which is used for network analysis and intelligence gathering. The interface is divided into several main sections:

- Left Panel:** A sidebar containing a search bar and a list of tool categories and specific tools, such as "Analyze DNS Records", "OSINT Event Summary", and "IP Geolocation".
- Top Panel:** A table displaying network information. The columns include "Source", "Destination", "Network Name", "Tech Contact", "Service Contact", "Status", "Maintenance", "Maintenance Level", "Maintenance Contact", "Maintenance Date", "Name Server", and "Set".
- Map Panel:** A satellite map showing a geographical area, likely the Pacific Northwest region, with a purple location marker.
- Bottom Panel:** A table displaying a list of network-related data points, including "Source", "Type", "Hostname", "Hostname Resolved", "IP", "Port", "Last Seen", and "Last Seen".

# OLYMPIA AT A GLANCE

The screenshot displays the OLYMPIA software interface with several active windows:

- Search Panel (Top Left):** Includes search filters for IP, date range (Start Date: April 12, 2012 00:00, End Date: May 02, 2012 23:59), and a list of tool categories.
- IP Information (Top Center):** A table listing IP addresses, their source, country, and network details.
 

IP	Source	Country	Network Name	Text Contact	Admin Contact	Abuse Contact	Status	Maintained By	Maintain Level	Maintain Domain	Maintain Rules	Name Server
APNIC (X)	APNIC	RU	2024-19781000-17	20242-AP	20242-AP		ALLOCATED PORTABLE	20242-AP	20242-APNIC-AP			
JF (S)	APNIC	RU	2024-19781000-17	20242-AP	20242-AP		ALLOCATED PORTABLE	20242-AP	20242-APNIC-AP			
IANA-BLOCK (Z)												
IANA-PRIVATE-001 (Z)												
APNIC (Z)												
RFC1918												
- IP Geolocation Map (Center):** A satellite map of Africa with a purple location pin in the central region. The map title is "May 10 2012 16:38:24 GMT".
- IP-IP Communication Summaries (Bottom Center):** A table showing communication data between IP addresses.
 

Selection A	Selection B	Count	Protocol	Port (Selection A)
██████████	██████████	6,403	TCP	80
██████████	██████████	6,401	TCP	8080
██████████	██████████	6,221	TCP	8080
██████████	██████████	6,221	TCP	8080
██████████	██████████	6,221	TCP	8080
- Geolocation and Network Information (ATLAS) (Bottom Right):** A table listing geolocation data.
 

IP	Request Status	Categories	Site Group	Entity Location	Entity Name
██████████	Approved	8028	RU	██████████	Russian Ministry of Internal Affairs
██████████	Approved	8028	RU	██████████	Russian Ministry of Internal Affairs
██████████	Approved	8028	RU	██████████	Russian Ministry of Internal Affairs
- Tool Menu (Right Side):** A vertical list of tools including Anonymizers (QUOVA), CNO Event Summaries (PROMETHEUS), Credentials (PEITHO), End Product Reports (SLINGSHOT), FFU Events (LEVITATE), GPRS Events (STRATOS), Geolocation (EVOLVE), Geolocation (GCHQ Geofusion), Geolocation Map (QUOVA), Geolocation and Network Information (ATLAS), GoC Network Information (ATLAS), IP-IP Communication Summaries (HYPERION), Ports Information (ATHENA), Reverse DNS (DANAUS), Router Configs (TIDALSURGE), Survey Information (BLACKPEARL), TDI Online Events (MARINA), TDI Online Events (PEITHO), Target Knowledge (STARSEARCH), Targeting Requests (PEPPERBOX), Tor Nodes (TRITON), Traceroutes (PACKAGEDGOODS/ARK), VPN Detailed Events (TOYGRIPPE), VPN Events (FRSARTUCK), VPN Events (TOYGRIPPE), VSAT Terminals (MASTERSHAKE), WHOIS Information (COEUS), and Web Forum Events (STALKER).



# OLYMPIA - AUTOMATION

The screenshot displays the OLYMPIA automation interface. The main workspace shows a workflow diagram with the following steps: TC Init, Dynamic Configuration, Contact Chains (MAINWAY): Date Range, MSISDN, Dummy (do nothing), Filter rows, Network Registration (GNDB): ITU E.164, Sort rows, and Tradecraft Navigator Output. A 'Phone Number Query' dialog box is open, showing the configuration for the 'Network Registration (GNDB): ITU E.164' step. The dialog includes a 'Parameter Mapping' table and a 'Result' column.

#	Field Name	Parameter Name	Parameter Type	Required	Bat
1	phoneNumber	ItuE164		yes	1

The 'Result' column contains a list of fields: Last Seen, Original Selector City, Original Selector Country, Original Selector Fips, and Original Selector Identity. The 'Get Fields' button is visible below the table.

On the right side, a 'Steps' panel lists various enrichment and data manipulation nodes, including: FASCIA PCS Events (SEDB): Date Range, MSISDN; FASCIA PCS Events (SEDB): Date Range, TMSI; FASCIA PCS Events (SEDB): DNR Selector, Date Range; FASCIA PSTN Events (SEDB): Date Range, ITU E.164; FFU Events (LEVITATE): Date Range, Free Text; FFU Events (LEVITATE): Date Range, IP Range; Forward DNS (DANAUS): Domain; Forward DNS (DANAUS): Hostname; Geolocation (EVLOLIVE): IP; Geolocation (GCHQ Geofusion): IP Range; Geolocation and Network Information (ATLAS): Date Range, IP Range; Geolocation and Network Information (QUOVA): ASN; Geolocation Map (QUOVA): Date Range, IP Range; GoC Network Information (ATLAS): IP Range; GPRS Events (STRATOS): Date Range, IP; GPRS Events (STRATOS): Date Range, IP\_2; GPRS Events (STRATOS): Date Range, LAIC; GPRS Events (STRATOS): Date Range, TDI; GPRS Events (STRATOS): DNR Selector, Date Range; GSM cells (OCTSKYWARD): LAIC; GSM cells (OCTSKYWARD): Mcc; IP-IP Communication Summaries (HYPERION): Date Range, IP Range; Mobile Network Operator (GNDB): IMSI; Mobile Network Operator (GNDB): LAIC; Network Registration (GNDB): ITU E.164; Open IP Ranges; Phone Book (TWINSERPENT): DNR Selector; Phone Book (TWINSERPENT): Free Text.

Numerous enrichment and data manipulation nodes  
Drag and drop each node  
Create links between nodes  
Hit the *Play* button

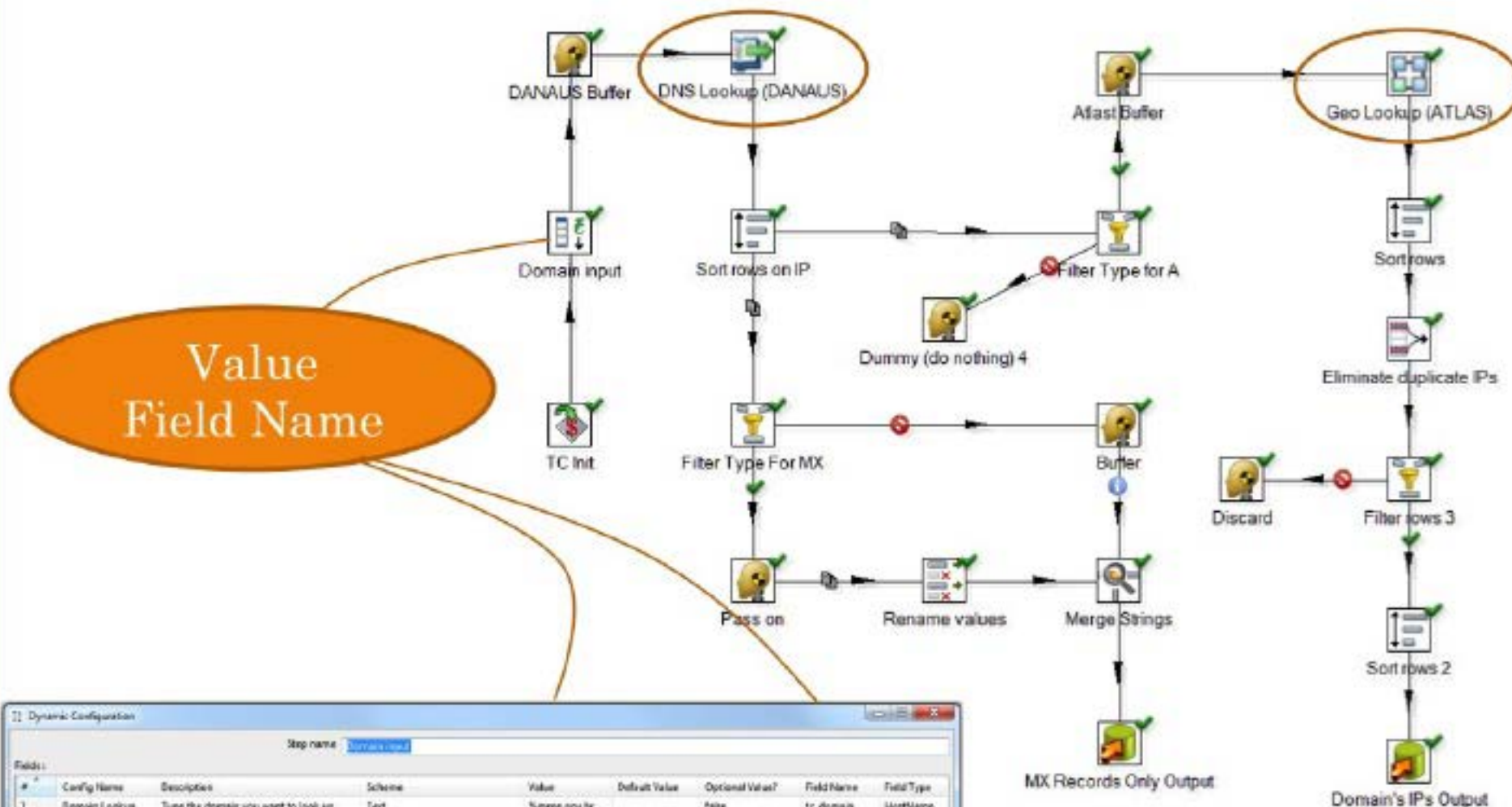
# ANALYSIS – CASE STUDY

What we know about the target:

- Domain: @mme.gov.br
- 9 DNR selectors
- Very little collection



# ANALYSIS – DETERMINE TARGET'S IPs AND ISPs



Value  
Field Name

Dynamic Configuration

Step name: **Domain input**

#	Config Name	Description	Schema	Value	Default Value	Optional Value?	Field Name	FieldType
1	Domain Lookup	Type the domain you want to look up	Text	funco.gov.tr		false	tc_domain	HostName

For more information, please visit the Wiki Page [https://wiki.cis-101.org/cwiki.php?Olympia/TX/Step/Dynamic\\_Configuration](https://wiki.cis-101.org/cwiki.php?Olympia/TX/Step/Dynamic_Configuration)

OK Cancel





# ANALYSIS – DETERMINE TARGET'S IPs AND ISPs

Hostname  
IPv4  
Country  
ASN  
Owner  
Carrier

## Mail Servers Output

Response_MX	Hostname	IPv4	Source	First Seen	Last Seen
correio.mme.gov.br	correio.mme.gov.br	[REDACTED]	EONBLUE	Wed Jun 17 06:04:23 GMT 2009	Mon Feb 15 12:40:53 GMT 2010
correio2.mme.gov.br	correio2.mme.gov.br	[REDACTED]	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011

## Domain's IPs Output

Type	Hostname	IPv4	IP Range	Country	ASN	Owner	Carrier	Source	First Seen	Last Seen
A	ns1.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Tue May 08 17:28:22 GMT 2012
A	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 22:09:50 GMT 2011	Sat May 05 10:35:50 GMT 2012
A	ns2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Tue May 08 17:28:22 GMT 2012
A	sv041.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Wed Apr 25 04:55:02 GMT 2012
A	correio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 16:26:42 GMT 2011	Wed May 02 21:11:17 GMT 2012
A	acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	ns1.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	correio2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Thu Feb 11 19:15:47 GMT 2010	Mon Dec 19 19:40:43 GMT 2011
A	ns2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Wed Sep 15 23:11:09 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	sv041.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Thu Mar 03 19:37:08 GMT 2011	Tue Dec 20 15:49:18 GMT 2011
A	prodem.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	sv041.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Wed Feb 10 12:53:14 GMT 2010	Tue Sep 07 09:24:15 GMT 2010
A	correio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Fri Feb 12 20:14:21 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	catalogo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	correio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	comite gestor da internet no brasil	sespro	QUOVA	Thu Feb 19 20:37:34 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	correio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	comite gestor da internet no brasil	sespro	QUOVA	Fri Mar 27 14:03:47 GMT 2000	Sat Nov 19 01:53:44 GMT 2011
A	urano.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	comite gestor da internet no brasil	sespro	QUOVA	Fri Mar 27 14:04:08 GMT 2000	Sat Nov 19 01:53:44 GMT 2011
A	teia.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	comite gestor da internet no brasil	sespro	QUOVA	Fri Mar 27 14:04:08 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	catalogo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	webpec.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	prodem.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	urano.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	teia.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Apr 20 11:02:46 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	correio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011

# ANALYSIS – DISCOVER TARGET'S PROXY

Dynamic Configuration

Step name: Input IP ranges

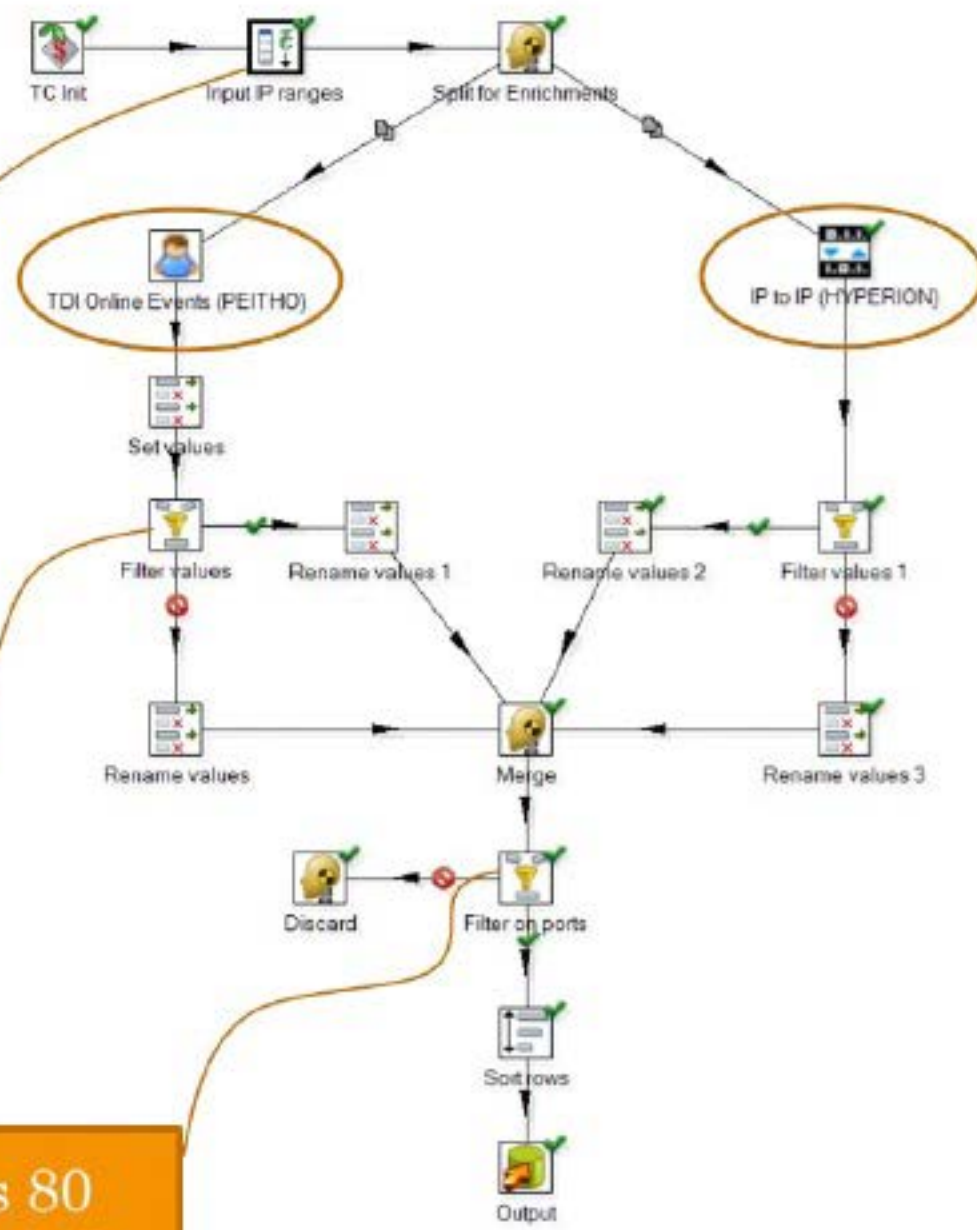
#	Config Name	Value	Default Value	Optional Value?	Field Name	Field Type
1	High IP	[REDACTED]		false	tc_highip	IP
2	IP Range	[REDACTED]		false	tc_iprange	iprange
3	Low IP	[REDACTED]		false	tc_lowip	IP

For more information, please go to [https://help.paloaltonetworks.com/step-dynamic-configuration](#)

OK Cancel

High IP  
Low IP  
IP Range

REMOTE PORT contains 80  
REMOTE PORT contains 443



# ANALYSIS – DISCOVER TARGET'S PROXY

## Target Proxy Output

entity IP	remote IP	remote port	entity port
[REDACTED]	[REDACTED]	6:443:TS (1);	6:47367:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (1);	6:27973:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (1);	6:48329:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (2);	6:47950:FC (1);6:483
[REDACTED]	[REDACTED]	6:443:TS (2);	6:54695:FC (1);6:435
[REDACTED]	[REDACTED]	6:443:TS (4);	6:31670:FC (1);6:343
[REDACTED]	[REDACTED]	6:443:TS (5);	6:1263:FC (1);6:4115
[REDACTED]	[REDACTED]	6:443:FS (12);	6:48927:TC (1);6:489
[REDACTED]	[REDACTED]	6:443:TS (179);6:80:1	6:26704:FC (1);6:267
[REDACTED]	[REDACTED]	6:443:TS (1);	6:11217:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (165);	6:12946:FC (1);6:152
[REDACTED]	[REDACTED]	6:443:TS (1);	6:60657:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (1);	6:45811:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (14);6:80:TS	6:19170:FC (2);6:536

Entity IP :

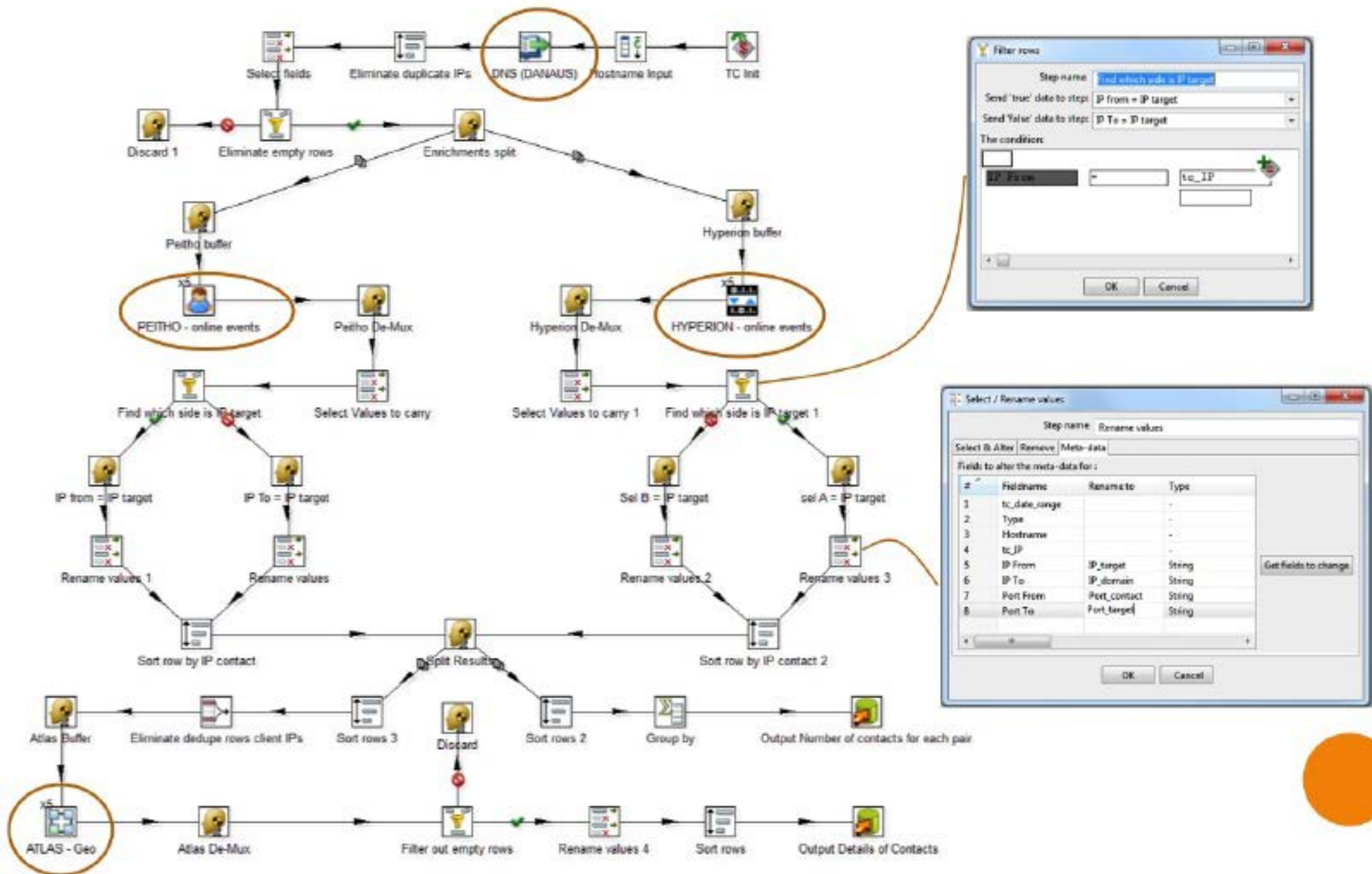
Remote IP : various

Remote Port : 443

Entity Port: various



# ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH



# ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH

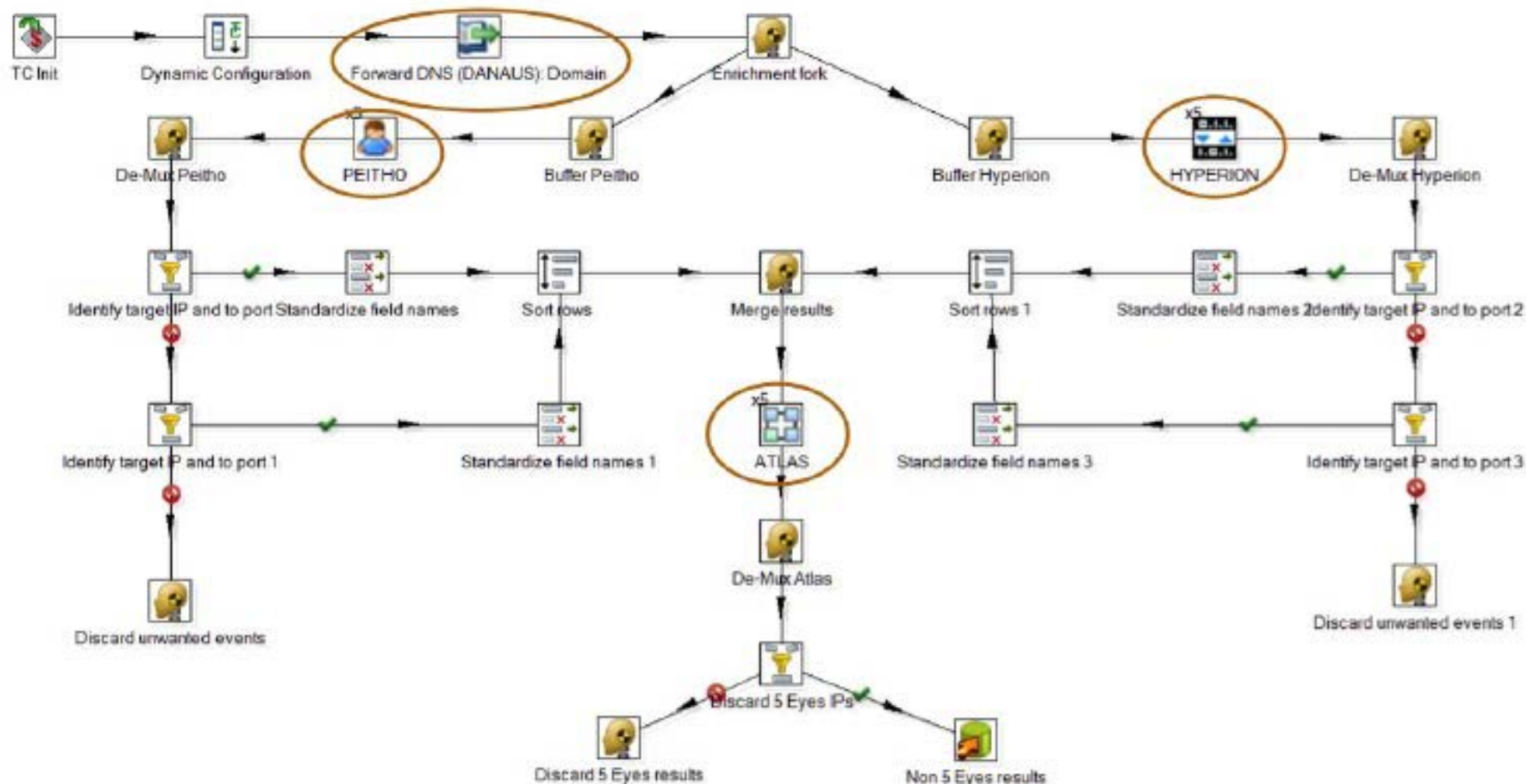
Hostname domain	IP domain	IP in contact with domain	Port used by IP domain	Port used by IP contact	Owner of IP contact	Carrier of IP contact	ASN of IP contact	Country of IP contact	IP range for IP contact
correio.mme.gov.br			6-25:TS (1);	6-61391:FC (1);	tse i net noc ip infrastructure	british telecommunications plc	5400 eritrea		
correio.mme.gov.br			6-25:TS (1);	6-61351:FC (1);	tse i net noc ip infrastructure	british telecommunications plc	5400 eritrea		
correio.mme.gov.br			6-25:TS (2);6-25:FS (1);	6-34251:FC (2)	tata communications	tata communications	6453 canada		
correio.mme.gov.br			6-25:TS (1);	6-28151:FC (1);	jtc	jordan telecommunications com	8697 jordan		
correio.mme.gov.br			6-25:TS (1);	6-2990:FC (1);	reassign to idc-dbw-idc customers loxinfo public company limite		9891 thailand		
correio.mme.gov.br			6-25:FS (1);	6-50072:TC (1);	internal network	international data exchange llc	12534 jordan		
correio.mme.gov.br			6-25:TS (1);	6-51934:FC (1);	pars online	parsonline	16322 iran		
correio.mme.gov.br			6-25:TS (1);	6-2295:FC (1);	dsl home subscribers	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-25:TS (1);	6-1795:FC (1);	dsl home subscribers	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-25:TS (1);	6-50329:FC (1);	dsl home subscribers	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-25:TS (1);	6-22433:FC (1);	saudnet saudi telecom compon	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-54356:TC	6-25:FS (128);	lweb dedicated hd	lweb technologies inc.	32613 canada		
correio.mme.gov.br			6-33907:TC	6-25:FS (22);	lweb dedicated hd	lweb technologies inc.	32613 canada		
correio.mme.gov.br			6-25:TS (4);	6-57773:FC	middle east internet company li	cyberia rajadh	34397 saudi arabia		
www.mme.gov.br			6-80:FS (1);	6-54791:TC (1);	adsl service	sahara net	41176 saudi arabia		

Hostname starting domain  
 IP starting domain  
 IP in contact with starting domain  
 Port used by starting domain  
 Port used by IP contact

Owner of IP contact  
 Carrier of IP contact  
 ASN of IP contact  
 Country of IP contact  
 IP range for IP contact



# ANALYSIS – IDENTIFY POTENTIAL MAN ON THE SIDE OPERATION AGAINST MY TARGET



# ANALYSIS – IDENTIFY POTENTIAL MAN ON THE SIDE OPERATION AGAINST MY TARGET

## Results

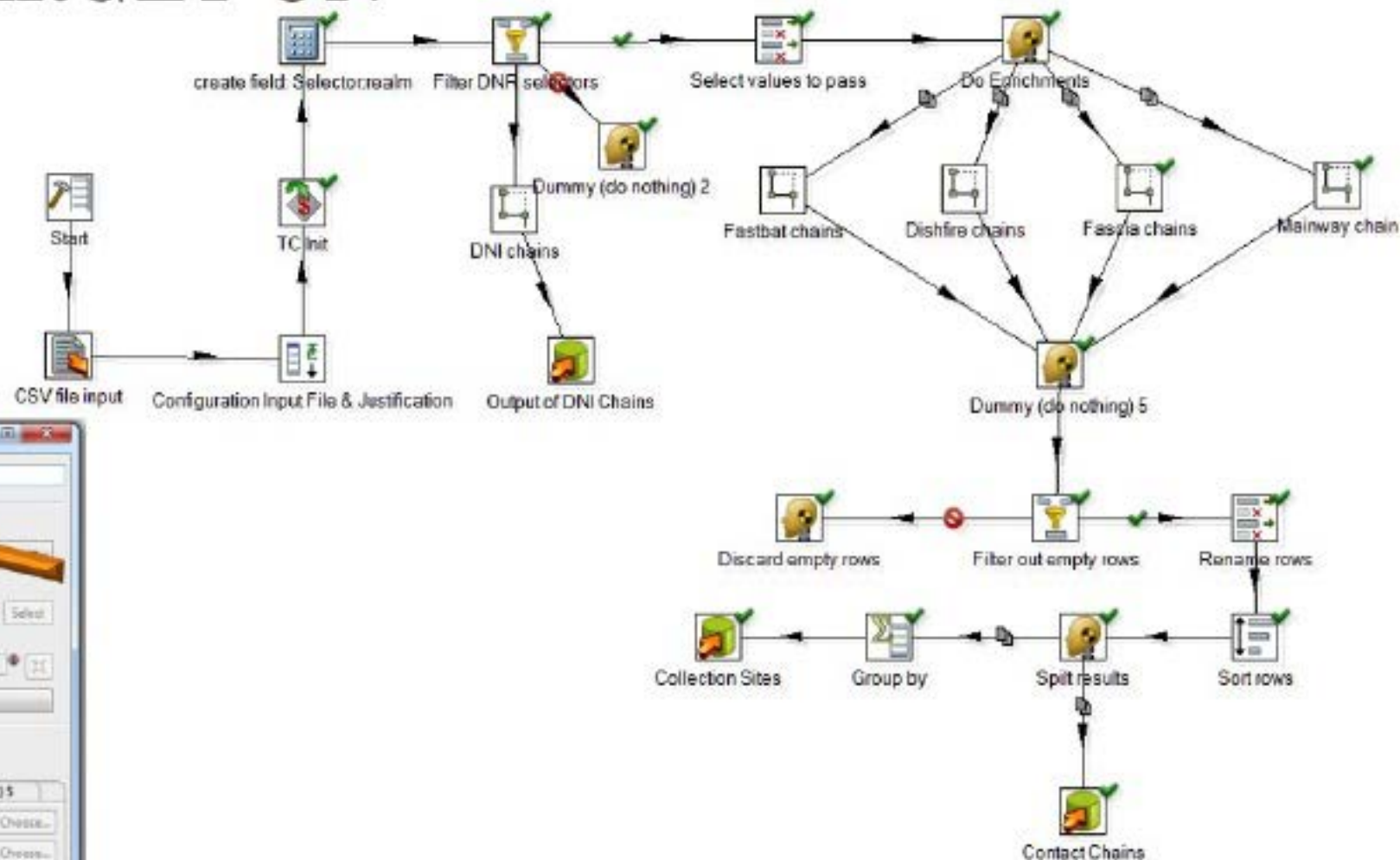
target_hostname	target	contact	target_port	contact_port	Case Notations	Country	Digraph
acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	6:41278:TC (1);	6:80:FS (1);	MA10099 (1);	brazil	br
acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	6:30141:TC (1);	6:80:FS (1);	MA10099 (1);	brazil	br

ASN contact	Country contact	# IPs contact
18881	brazil	26
7738	brazil	11
26599	brazil	6
19182	brazil	3
10429	brazil	2
27717	brazil	2
53006	brazil	2
14080	colombia	1
16735	brazil	1
32613	brazil	1
52972	brazil	1
8151	mexico	1

ASN contact	Country contact	# IPs contact
18881	brazil	15
26599	brazil	9
10429	brazil	7
16735	brazil	5
18479	brazil	3
45774	india	3
7738	brazil	3
19182	brazil	2
27699	brazil	2
13878	brazil	1
14080	colombia	1
16509	brazil	1
17379	brazil	1
28311	brazil	1
28670	brazil	1
32613	brazil	1
4808	china	1
53018	brazil	1
53070	brazil	1
9829	india	1

Source	Type	Hostname	Hostname Decoded	IPs
EONBLUE	A	worle.net.br	worle.net.br	[REDACTED]
EONBLUE	A	staghin.com.br	staghin.com.br	[REDACTED]
EONBLUE	A	transformadovestib.com.br	transformadovestib.com.br	[REDACTED]
EONBLUE	A	geofora.br	geofora.br	[REDACTED]
EONBLUE	A	maytras.com.br	maytras.com.br	[REDACTED]
EONBLUE	A	fatecapes.edu.br	fatecapes.edu.br	[REDACTED]
EONBLUE	A	abclor.com.br	abclor.com.br	[REDACTED]
EONBLUE	A	telebreed.org.br	telebreed.org.br	[REDACTED]
EONBLUE	A	afabip.com.br	afabip.com.br	[REDACTED]
EONBLUE	A	advoc.com.br	advoc.com.br	[REDACTED]
EONBLUE	A	metajato.com.br	metajato.com.br	[REDACTED]
EONBLUE	A	guiafona.com.br	guiafona.com.br	[REDACTED]
EONBLUE	A	atq.com.br	atq.com.br	[REDACTED]
EONBLUE	A	flapress.com.br	flapress.com.br	[REDACTED]
EONBLUE	A	mhrvagens.com.br	mhrvagens.com.br	[REDACTED]
EONBLUE	A	stephendot.com.br	stephendot.com.br	[REDACTED]
EONBLUE	A	2housemoves.com.br	2housemoves.com.br	[REDACTED]
EONBLUE	A	thats.com.br	thats.com.br	[REDACTED]
EONBLUE	A	gafina.com.br	gafina.com.br	[REDACTED]
EONBLUE	A	edpoh.com.br	edpoh.com.br	[REDACTED]
EONBLUE	A	institutoepcc.org	institutoepcc.org	[REDACTED]

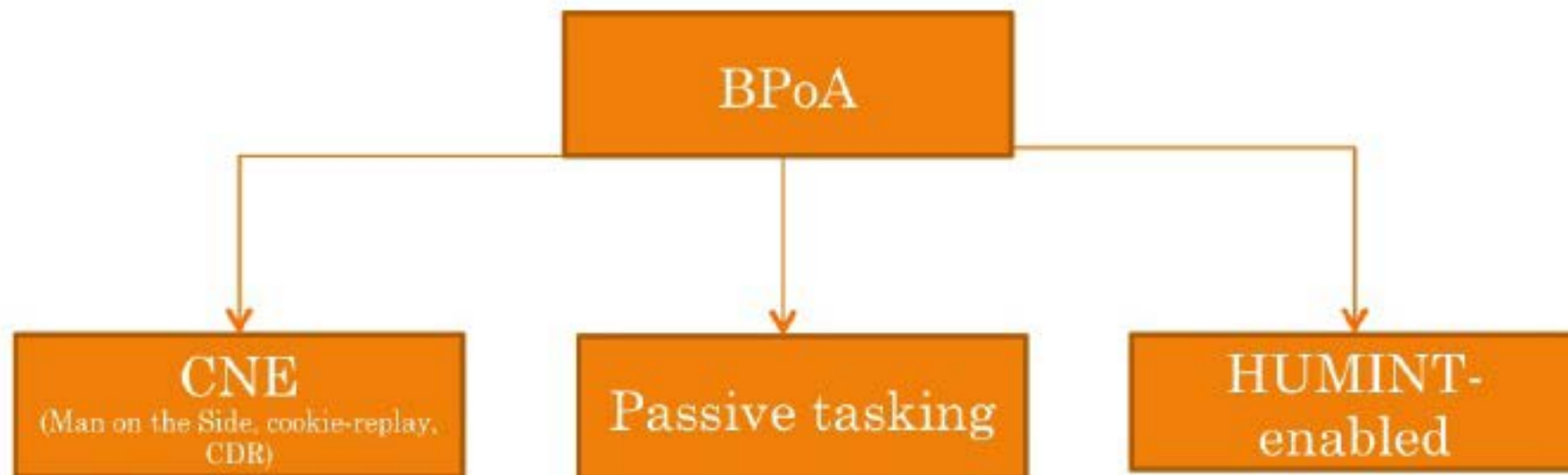
# ANALYSIS – DISCOVER CONTACTS OF MY TARGET AND COLLECTION SITES I SEE MY TARGET ON





## SUMMARY

Based on the information collected, I am better positioned to analyse my target's telecoms environment.



## MOVING FORWARD

- I have identified MX servers which have been targeted to passive collection by the Intel analysts, who are assessing the value, provenance, etc. of the traffic generated by the mail servers.
- I am working with TAO to further examine the possibility for a Man on the Side operation.
- Based on the network information gathered, the NAC has started a BPoA analysis on the MME.

