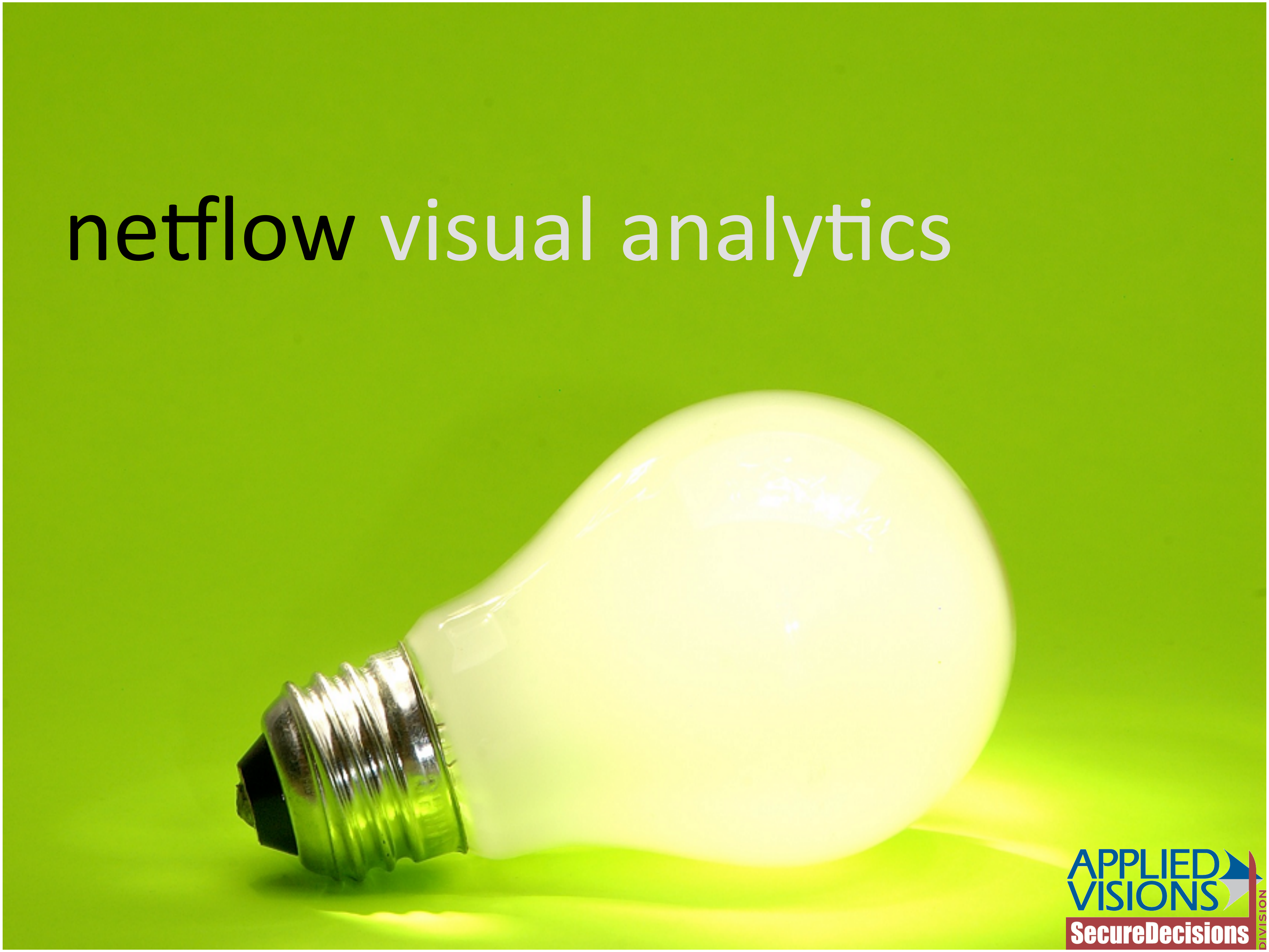
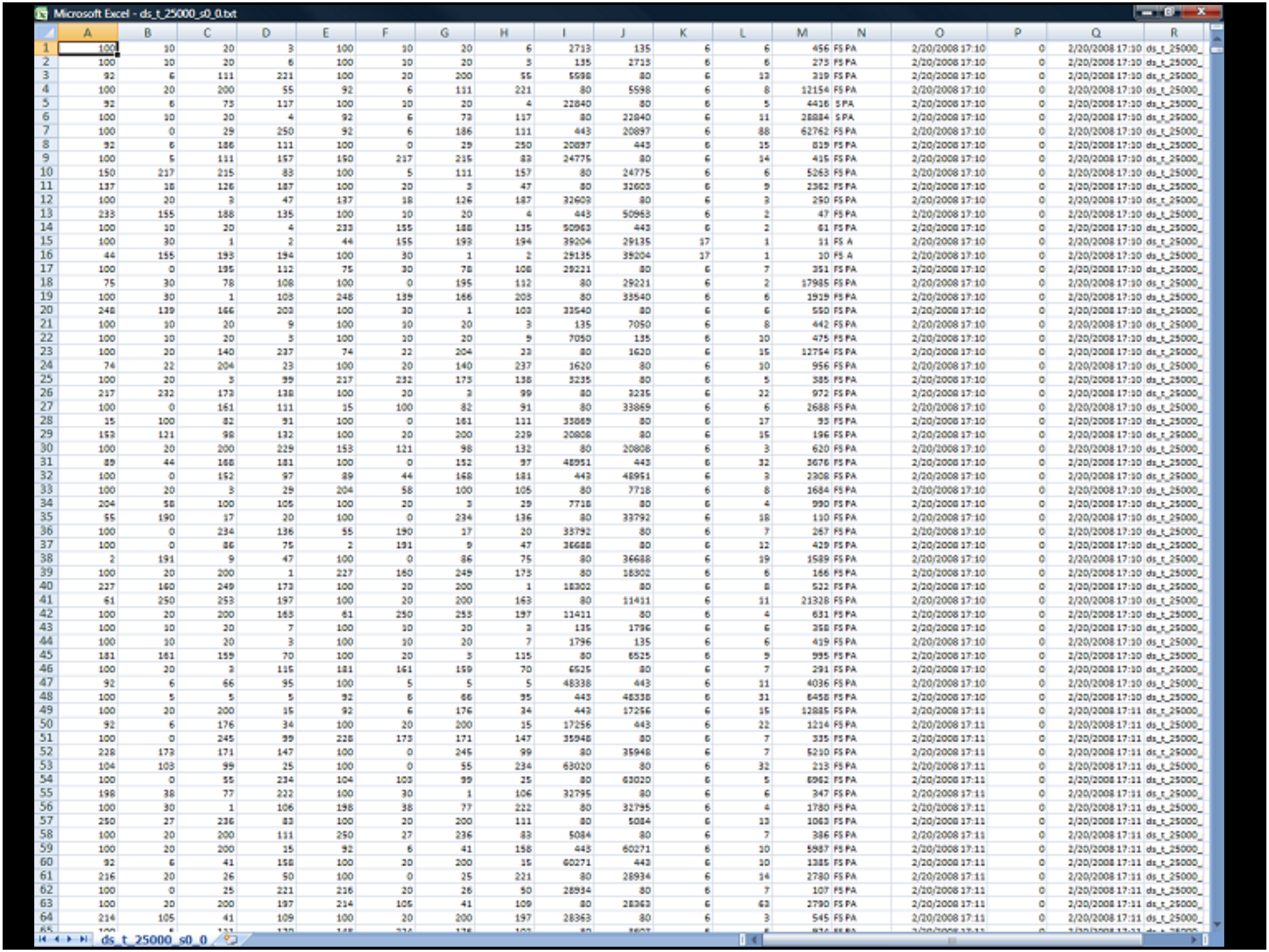
netflow visual analytics



APPLIED VISIONS
SecureDecisions
DIVISION

1,542,761,868

flows per day at US-CERT

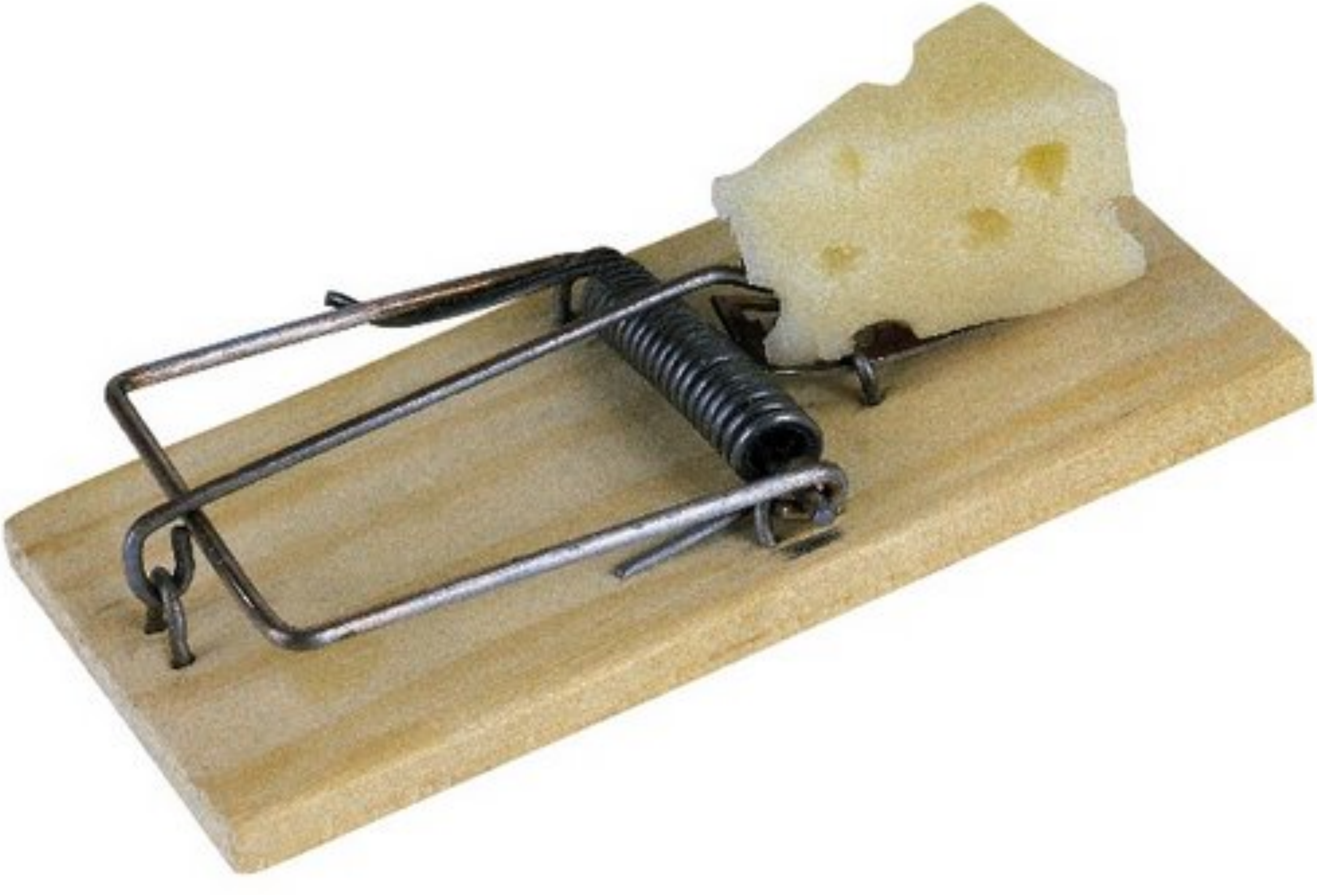


Microsoft Excel - ds_t_25000_s0_0.txt

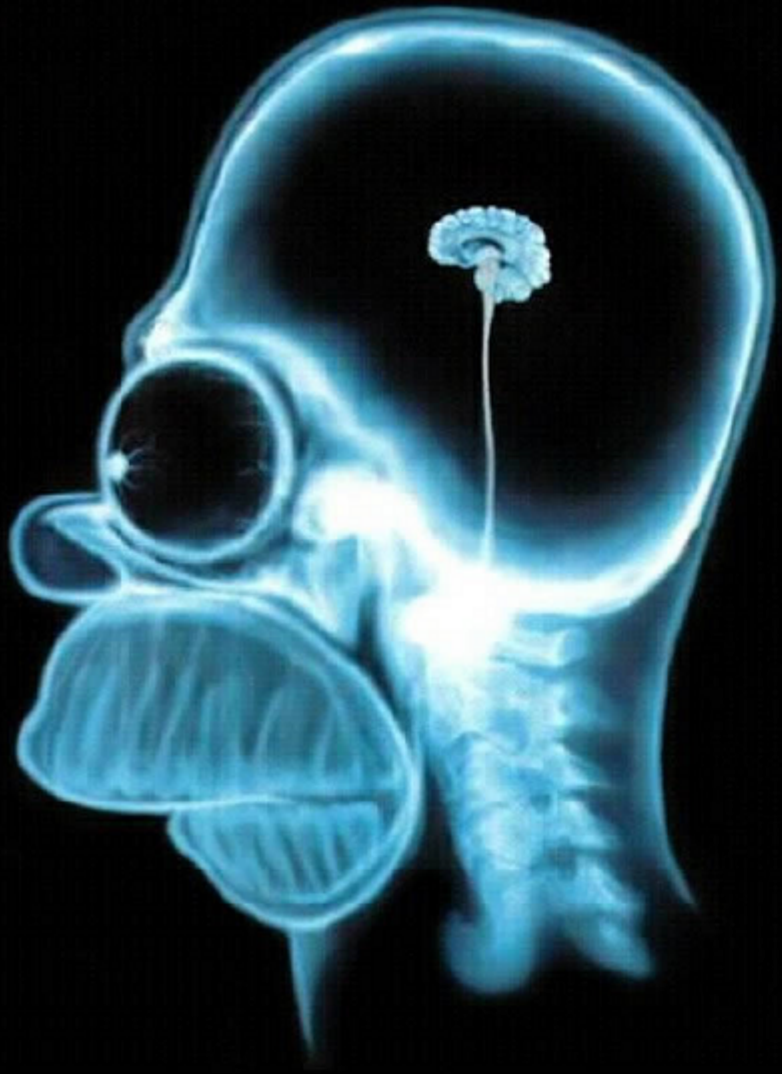
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	100	10	20	3	100	10	20	6	2713	135	6	6	456	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
2	100	10	20	6	100	10	20	3	135	2713	6	6	273	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
3	92	6	111	221	100	20	200	55	5598	80	6	13	319	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
4	100	20	200	55	92	6	111	221	80	5598	6	8	12154	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
5	92	6	73	117	100	10	20	4	22840	80	6	5	4416	S PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
6	100	10	20	4	92	6	73	117	80	22840	6	11	28884	S PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
7	100	0	29	250	92	6	186	111	443	20897	6	88	62762	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
8	92	6	186	111	100	0	29	250	20897	443	6	15	819	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
9	100	5	111	157	150	217	215	83	24775	80	6	14	415	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
10	150	217	215	83	100	5	111	157	80	24775	6	6	5263	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
11	137	18	126	187	100	20	3	47	80	32603	6	9	2362	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
12	100	20	3	47	137	18	126	187	32603	80	6	3	250	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
13	233	155	188	135	100	10	20	4	443	50963	6	2	47	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
14	100	10	20	4	233	155	188	135	50963	443	6	2	61	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
15	100	30	1	2	44	155	193	194	39204	29135	17	1	11	FS A	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
16	44	155	193	194	100	30	1	2	29135	39204	17	1	10	FS A	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
17	100	0	195	112	75	30	78	108	29221	80	6	7	351	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
18	75	30	78	108	100	0	195	112	80	29221	6	2	17985	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
19	100	30	1	103	248	139	166	203	80	33540	6	6	1919	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
20	248	139	166	203	100	30	1	103	33540	80	6	6	550	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
21	100	10	20	9	100	10	20	3	135	7050	6	8	442	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
22	100	10	20	3	100	10	20	9	7050	135	6	10	475	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
23	100	20	140	237	74	22	204	23	80	1620	6	15	12754	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
24	74	22	204	23	100	20	140	237	1620	80	6	10	956	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
25	100	20	3	99	217	232	173	138	3235	80	6	5	385	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
26	217	232	173	138	100	20	3	99	80	3235	6	22	972	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
27	100	0	161	111	15	100	82	91	80	33869	6	6	2688	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
28	15	100	82	91	100	0	161	111	33869	80	6	17	93	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
29	153	121	98	132	100	20	200	229	20808	80	6	15	196	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
30	100	20	200	229	153	121	98	132	80	20808	6	3	620	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
31	89	44	168	181	100	0	152	97	48951	443	6	32	3676	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
32	100	0	152	97	89	44	168	181	443	48951	6	3	2308	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
33	100	20	3	29	204	58	100	105	80	7718	6	8	1684	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
34	204	58	100	105	100	20	3	29	7718	80	6	4	990	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
35	55	190	17	20	100	0	234	136	80	33792	6	18	110	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
36	100	0	234	136	55	190	17	20	33792	80	6	7	267	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
37	100	0	86	75	2	191	9	47	36688	80	6	12	429	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
38	2	191	9	47	100	0	86	75	80	36688	6	19	1589	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
39	100	20	200	1	227	160	249	173	80	18302	6	6	166	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
40	227	160	249	173	100	20	200	1	18302	80	6	8	522	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
41	61	250	253	197	100	20	200	163	80	11411	6	11	21328	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
42	100	20	200	163	61	250	253	197	11411	80	6	4	631	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
43	100	10	20	7	100	10	20	3	135	1796	6	6	358	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
44	100	10	20	3	100	10	20	7	1796	135	6	6	419	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
45	181	161	159	70	100	20	3	115	80	6525	6	9	995	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
46	100	20	3	115	181	161	159	70	6525	80	6	7	291	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
47	92	6	66	95	100	5	5	5	48338	443	6	11	4036	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
48	100	5	5	5	92	6	66	95	443	48338	6	31	6458	FS PA	2/20/2008 17:10	0	2/20/2008 17:10	ds_t_25000_
49	100	20	200	15	92	6	176	34	443	17256	6	15	12885	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
50	92	6	176	34	100	20	200	15	17256	443	6	22	1214	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
51	100	0	245	99	228	173	171	147	35948	80	6	7	335	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
52	228	173	171	147	100	0	245	99	80	35948	6	7	5210	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
53	104	103	99	25	100	0	55	234	63020	80	6	32	213	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
54	100	0	55	234	104	103	99	25	80	63020	6	5	6962	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
55	198	38	77	222	100	30	1	106	32795	80	6	6	347	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
56	100	30	1	106	198	38	77	222	80	32795	6	4	1780	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
57	250	27	236	83	100	20	200	111	80	5084	6	13	1063	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
58	100	20	200	111	250	27	236	83	5084	80	6	7	386	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
59	100	20	200	15	92	6	41	158	443	60271	6	10	5987	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
60	92	6	41	158	100	20	200	15	60271	443	6	10	1385	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
61	216	20	26	50	100	0	25	221	80	28934	6	14	2780	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
62	100	0	25	221	216	20	26	50	28934	80	6	7	107	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
63	100	20	200	197	214	105	41	109	80	28363	6	63	2790	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_
64	214	105	41	109	100	20	200	197	28363	80	6	3	545	FS PA	2/20/2008 17:11	0	2/20/2008 17:11	ds_t_25000_

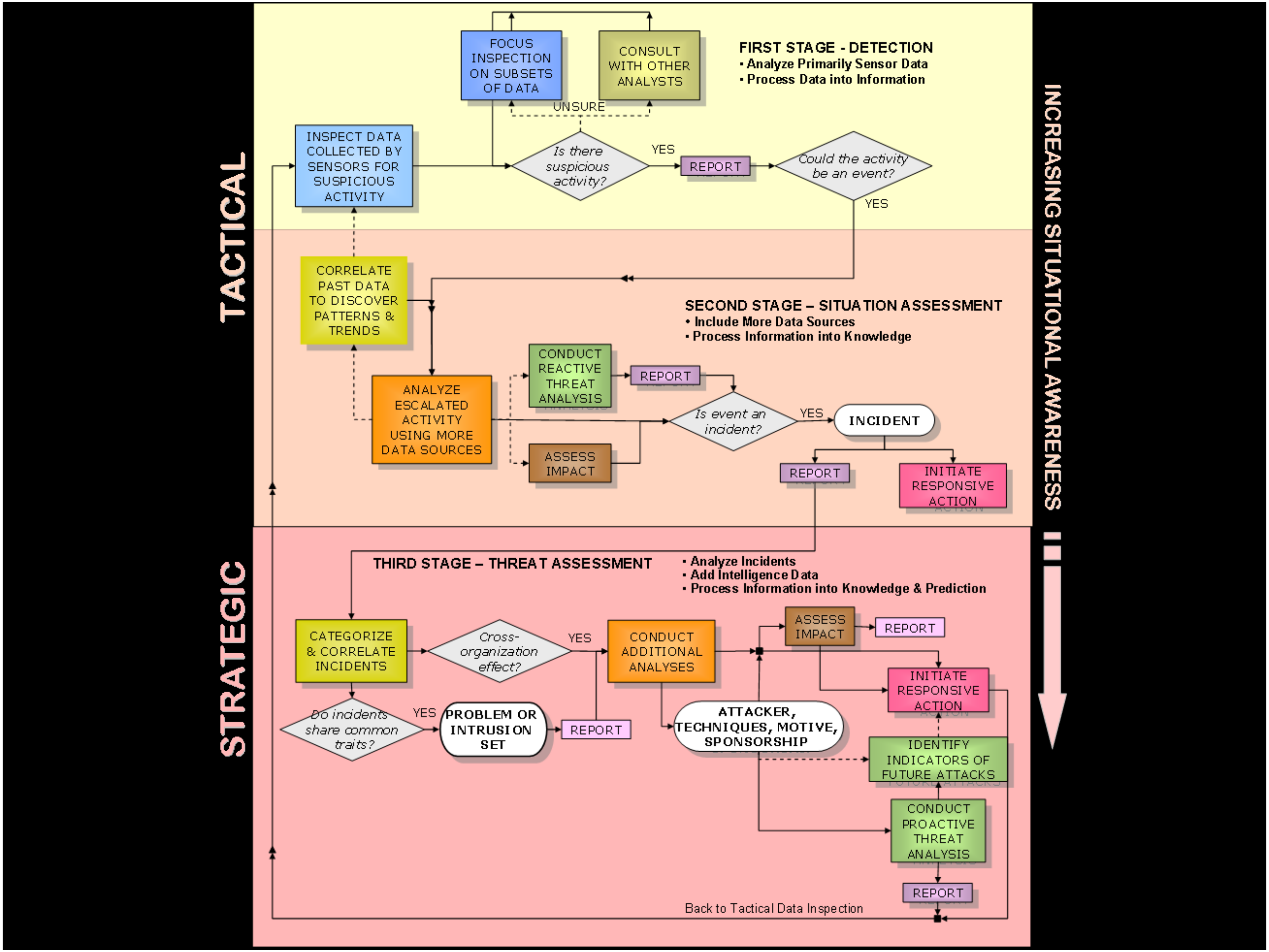
see the needle?

how can we do better?



cognitive task analysis





TACTICAL

STRATEGIC

INCREASING SITUATIONAL AWARENESS

FIRST STAGE - DETECTION

- Analyze Primarily Sensor Data
- Process Data into Information

INSPECT DATA COLLECTED BY SENSORS FOR SUSPICIOUS ACTIVITY

Is there suspicious activity?

UNSURE

FOCUS INSPECTION ON SUBSETS OF DATA

CONSULT WITH OTHER ANALYSTS

YES

REPORT

Could the activity be an event?

YES

SECOND STAGE – SITUATION ASSESSMENT

- Include More Data Sources
- Process Information into Knowledge

CORRELATE PAST DATA TO DISCOVER PATTERNS & TRENDS

ANALYZE ESCALATED ACTIVITY USING MORE DATA SOURCES

CONDUCT REACTIVE THREAT ANALYSIS

REPORT

ASSESS IMPACT

Is event an incident?

YES

INCIDENT

REPORT

INITIATE RESPONSIVE ACTION

THIRD STAGE – THREAT ASSESSMENT

- Analyze Incidents
- Add Intelligence Data
- Process Information into Knowledge & Prediction

CATEGORIZE & CORRELATE INCIDENTS

Cross-organization effect?

YES

CONDUCT ADDITIONAL ANALYSES

Do incidents share common traits?

YES

PROBLEM OR INTRUSION SET

REPORT

ASSESS IMPACT

REPORT

INITIATE RESPONSIVE ACTION

ATTACKER, TECHNIQUES, MOTIVE, SPONSORSHIP

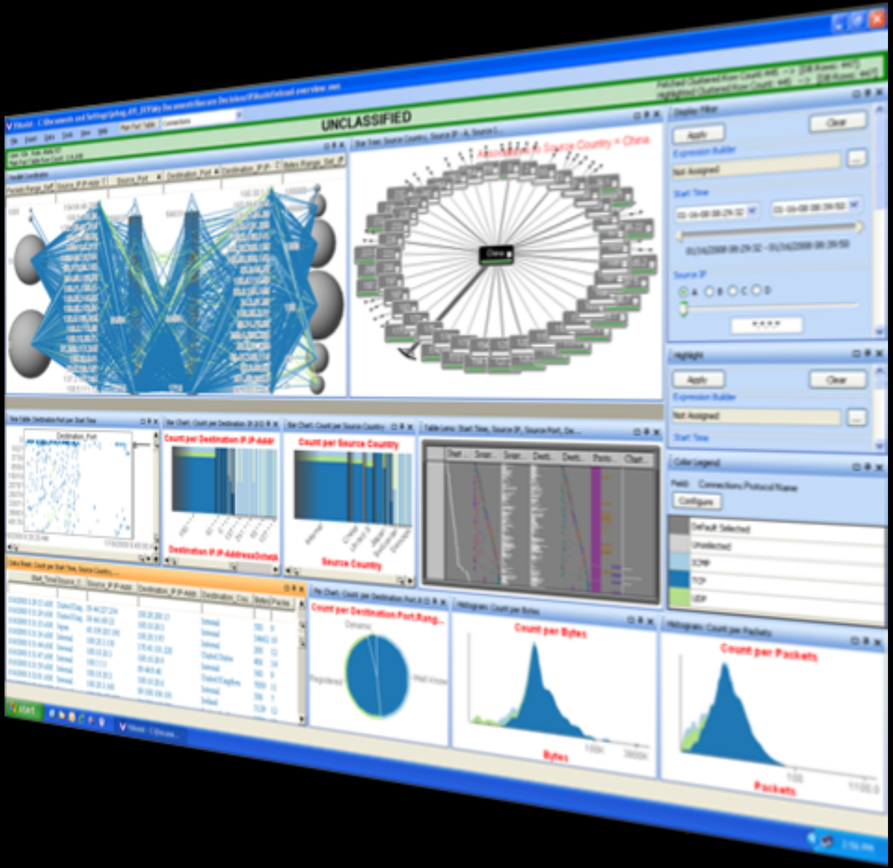
IDENTIFY INDICATORS OF FUTURE ATTACKS

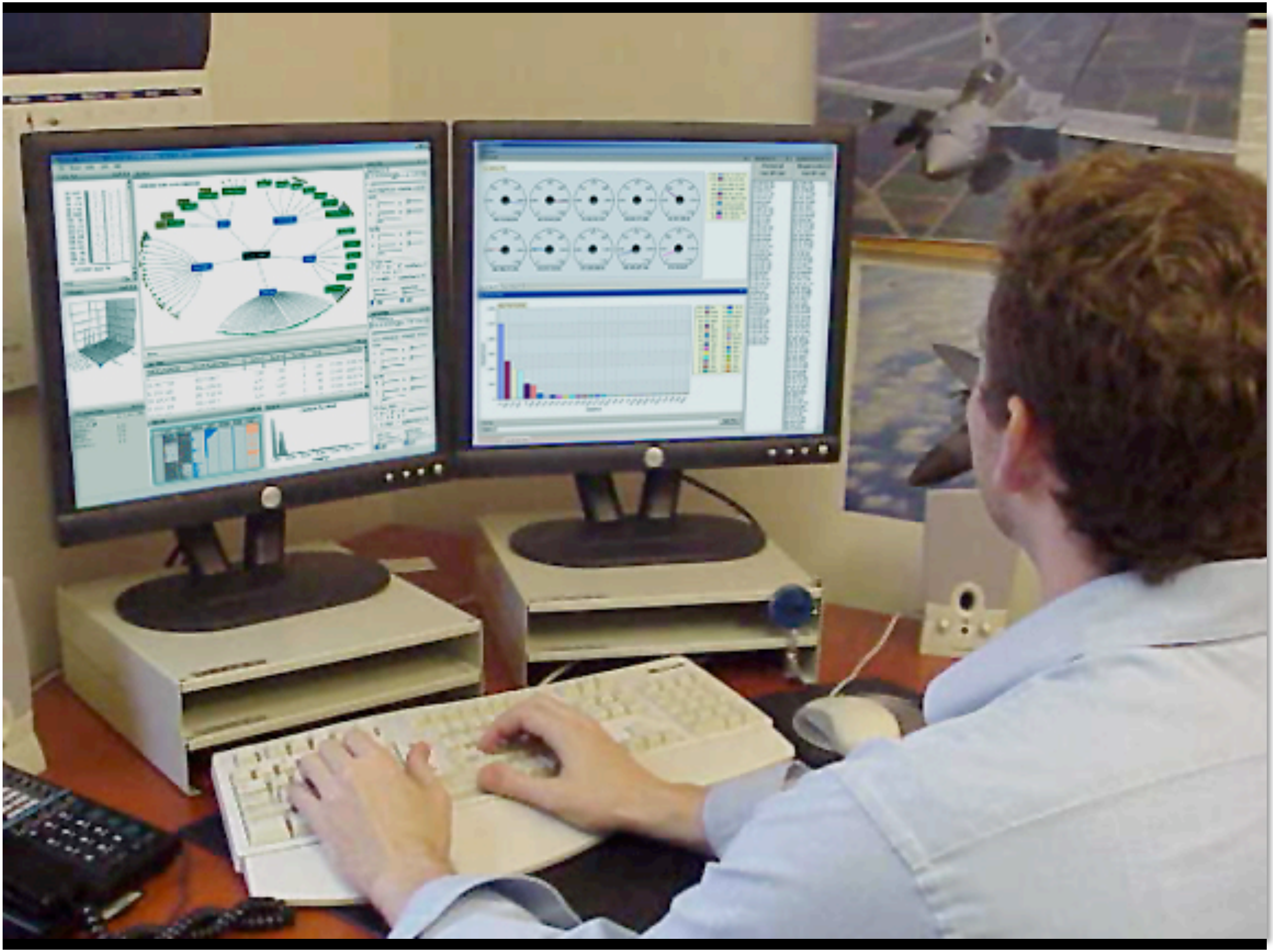
CONDUCT PROACTIVE THREAT ANALYSIS

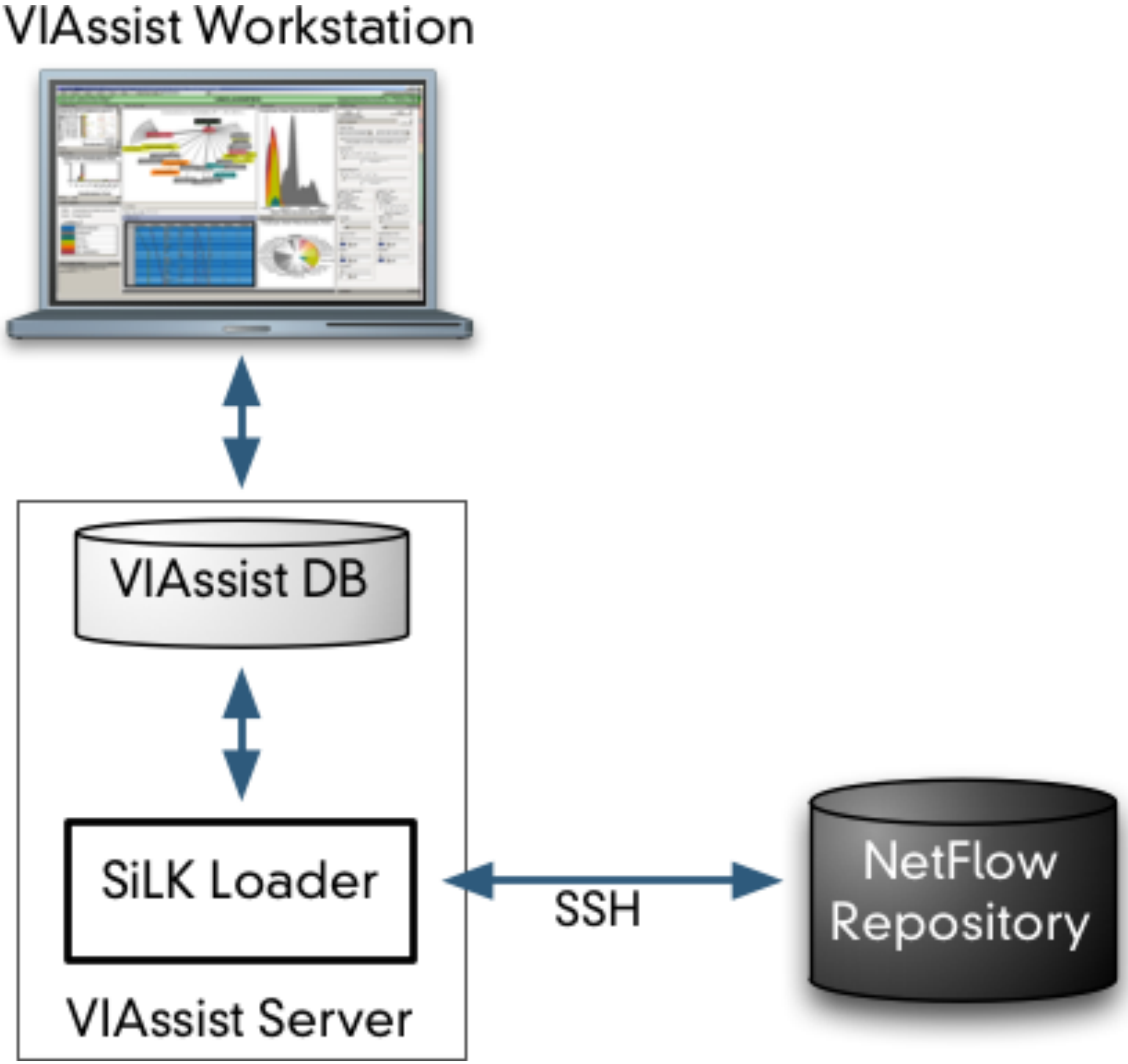
REPORT

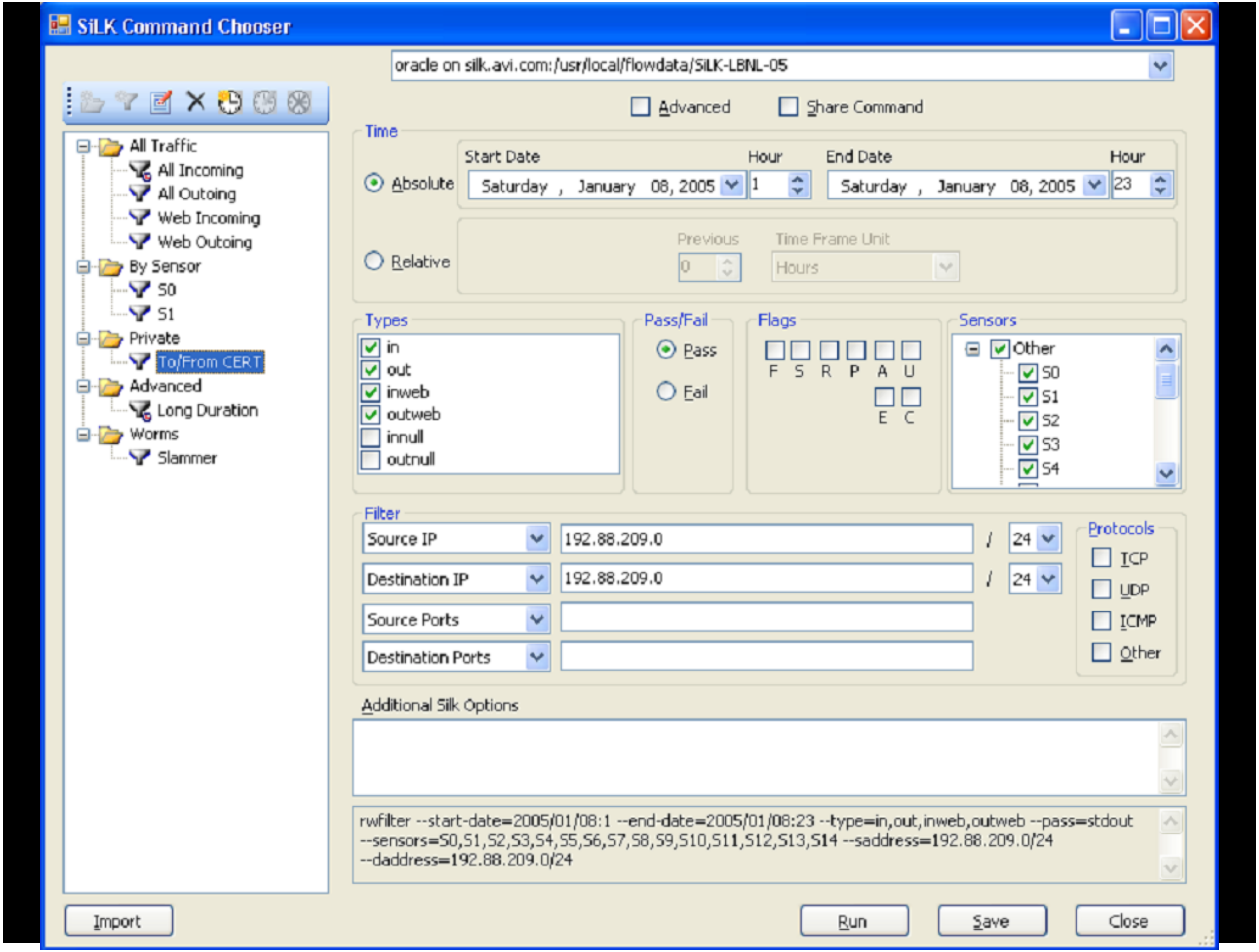
Back to Tactical Data Inspection

VIASSIST


UNCLASSIFIED
Count per Destination IP.IP-Addr
Destination IP.IP-AddressOctets
Count per Source Country
Source Country
Count per Destination Port.Rang...
Count per Bytes
Bytes
Count per Packets
Packets
Apply
Clear
Not Assigned
Start Time
Source IP
Color Legend
Configure
Default Selected
Unselected
ICMP
TCP
UDP




VIAssist Workstation
VIAssist DB
SiLK Loader
VIAssist Server
SSH
NetFlow Repository



oracle on silk.avi.com:/usr/local/flowdata/SiLK-LBNL-05

□ Advanced □ Share Command

Time

● Absolute

Start Date	Hour	End Date	Hour
Saturday , January 08, 2005	1	Saturday , January 08, 2005	23

○ Relative Previous 0 Time Frame Unit Hours

Types

☑ in
☑ out
☑ inweb
☑ outweb
□ innull
□ outnull

Pass/Fail

● Pass
○ Fail

Flags

□ F □ S □ R □ P □ A □ U □ E □ C

Sensors

☑ Other
☑ S0
☑ S1
☑ S2
☑ S3
☑ S4

Filter

Source IP	192.88.209.0	/	24
Destination IP	192.88.209.0	/	24
Source Ports			
Destination Ports			

Protocols

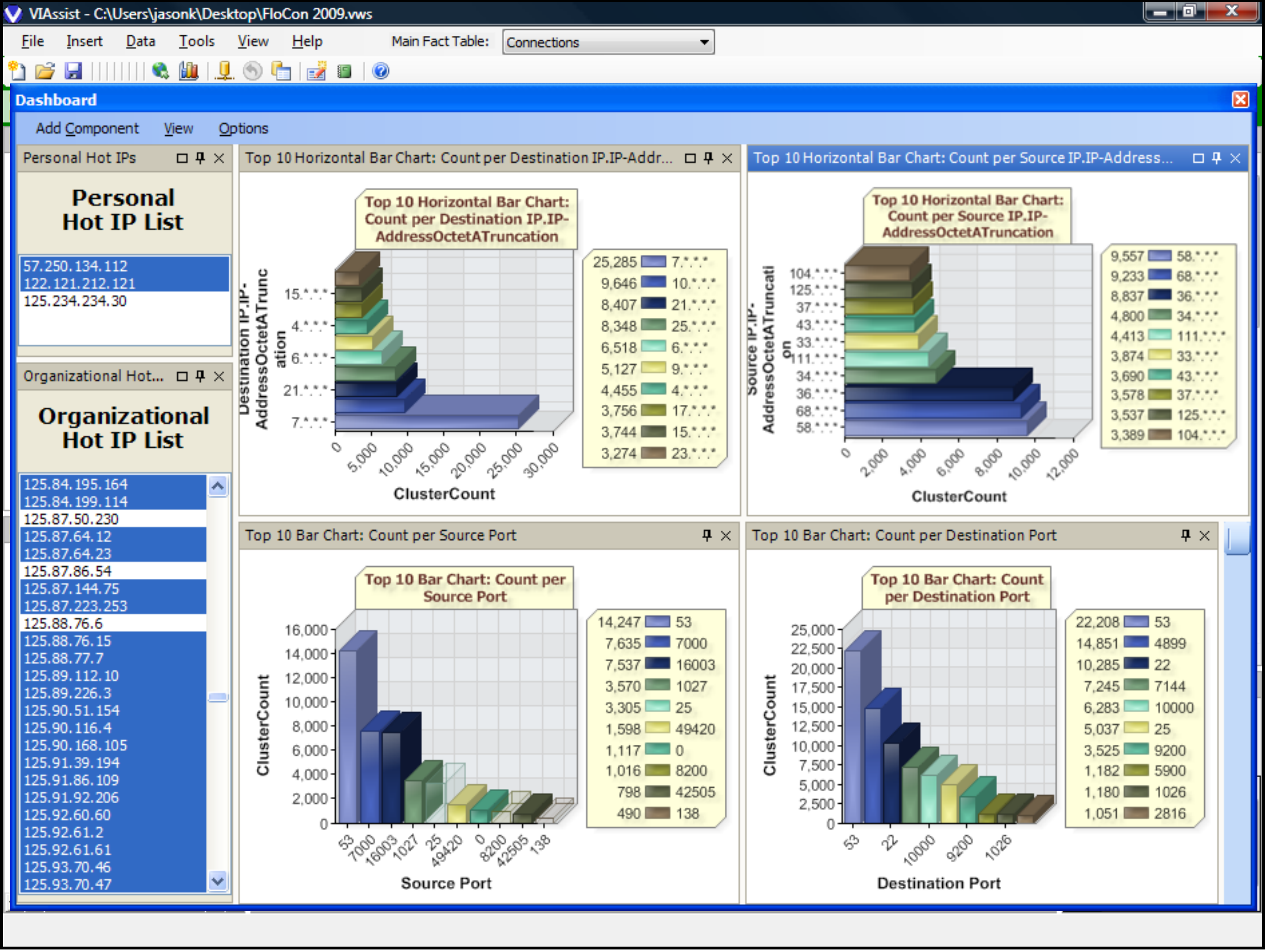
□ TCP
□ UDP
□ ICMP
□ Other

Additional Silk Options

```
rwfilter --start-date=2005/01/08:1 --end-date=2005/01/08:23 --type=in,out,inweb,outweb --pass=stdout
--sensors=S0,S1,S2,S3,S4,S5,S6,S7,S8,S9,S10,S11,S12,S13,S14 --saddress=192.88.209.0/24
--daddress=192.88.209.0/24
```

smart aggregation

2 million unfiltered flows



VIAssist - C:\Users\jasonk\Desktop\FloCon 2009.vws

Main Fact Table: Connections

Dashboard

Personal Hot IPs

Personal Hot IP List

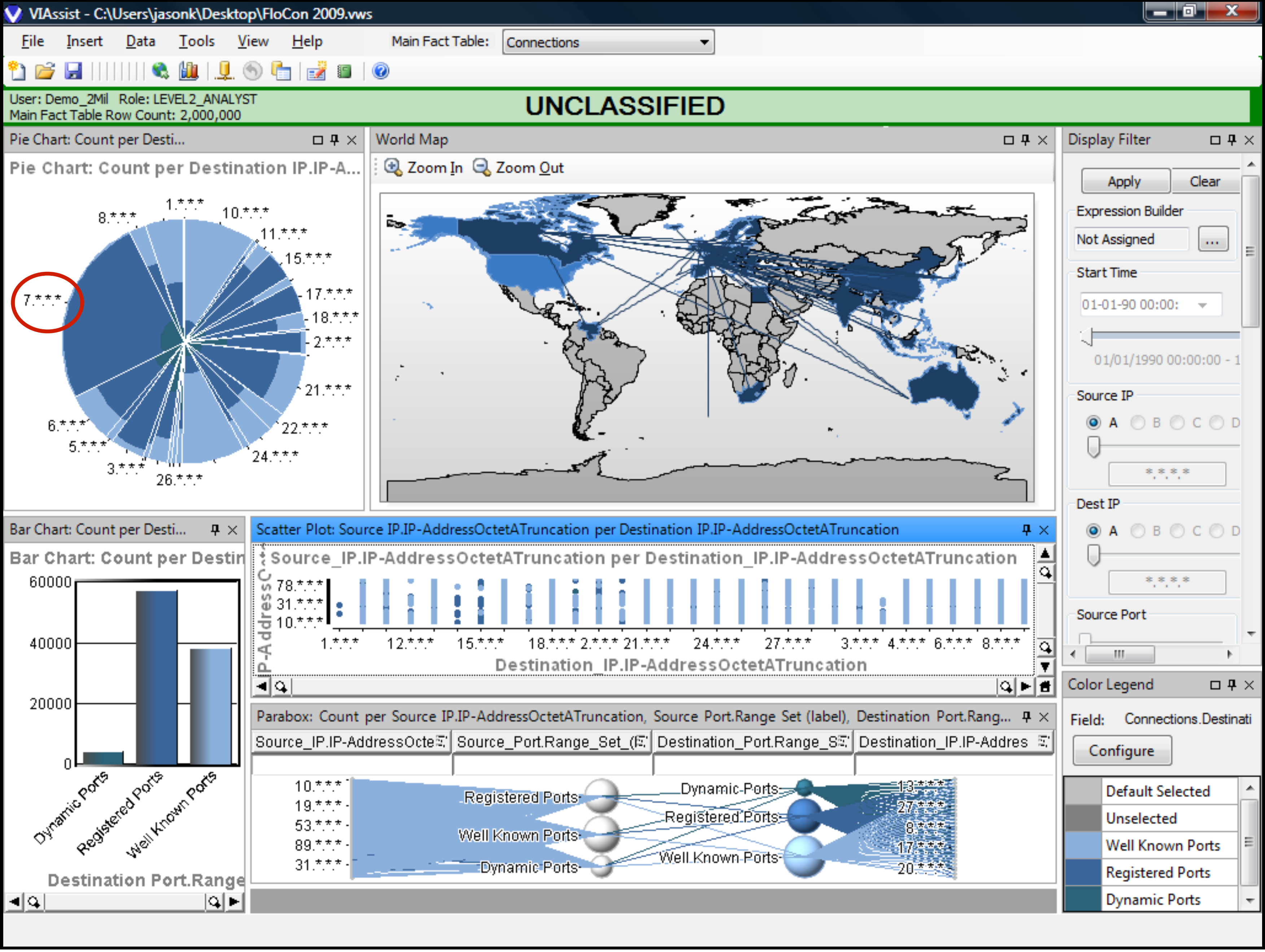
- 57.250.134.112
- 122.121.212.121
- 125.234.234.30

Organizational Hot...

Organizational Hot IP List

- 125.84.195.164
- 125.84.199.114
- 125.87.50.230
- 125.87.64.12
- 125.87.64.23
- 125.87.86.54
- 125.87.144.75
- 125.87.223.253
- 125.88.76.6
- 125.88.76.15
- 125.88.77.7
- 125.89.112.10
- 125.89.226.3
- 125.90.51.154
- 125.90.116.4
- 125.90.168.105
- 125.91.39.194
- 125.91.86.109
- 125.91.92.206
- 125.92.60.60
- 125.92.61.2
- 125.92.61.61
- 125.93.70.46
- 125.93.70.47

2 million unfiltered flows



VIAssist - C:\Users\jasonk\Desktop\FloCon 2009.vws

Main Fact Table: Connections

User: Demo_2Mil Role: LEVEL2_ANALYST
Main Fact Table Row Count: 2,000,000

UNCLASSIFIED

Expression Builder: Not Assigned

Start Time: 01-01-90 00:00:
01/01/1990 00:00:00 - 1

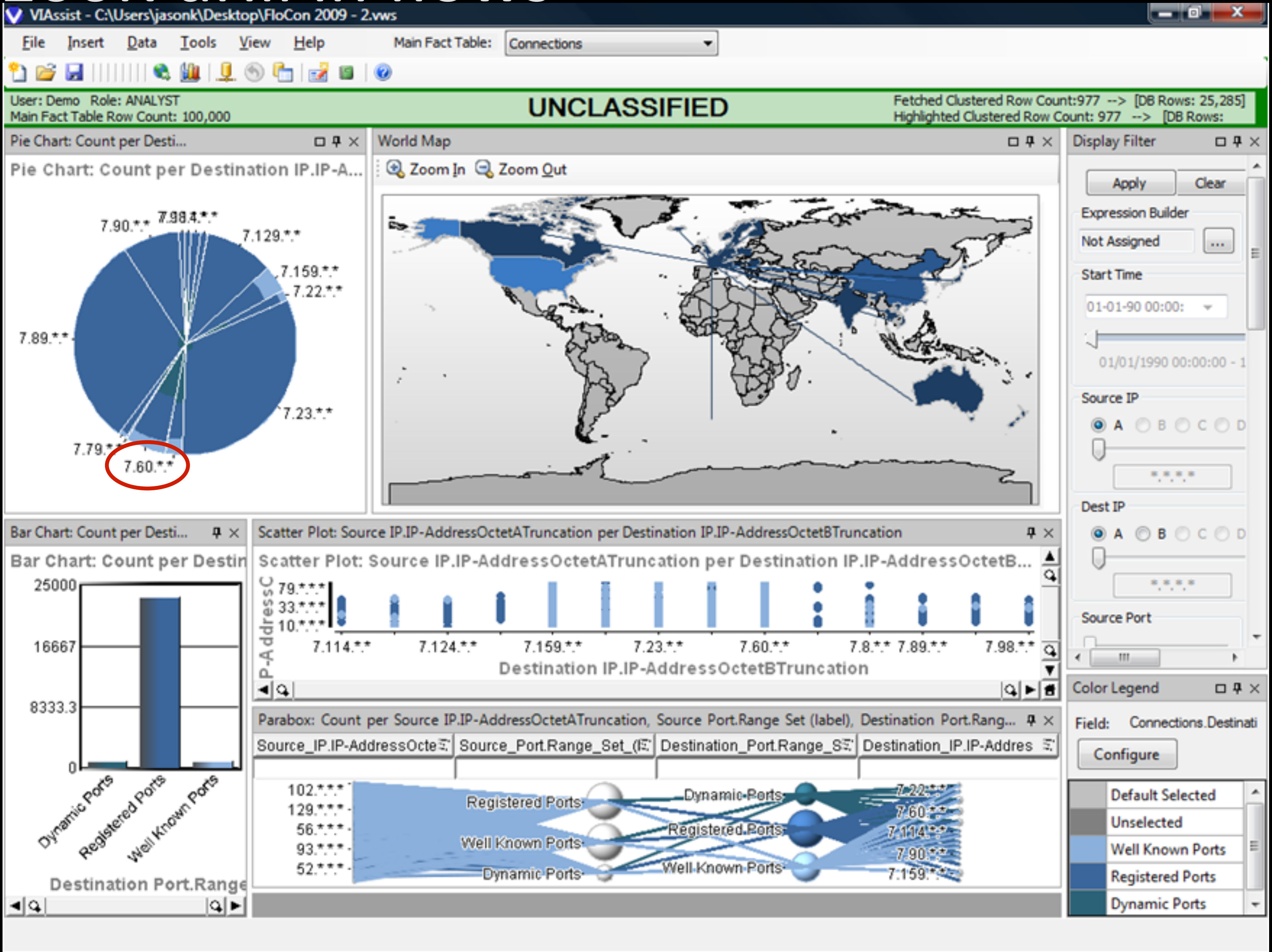
Source IP: ● A ○ B ○ C ○ D
..*.*

Dest IP: ● A ○ B ○ C ○ D
..*.*

Color Legend
Field: Connections.Destinati

▨	Default Selected
▨	Unselected
▨	Well Known Ports
▨	Registered Ports
▨	Dynamic Ports

100K drill in flows



VIAssist - C:\Users\jasonk\Desktop\FloCon 2009 - 2.vws

Main Fact Table: Connections

User: Demo Role: ANALYST
Main Fact Table Row Count: 100,000

UNCLASSIFIED

Fetched Clustered Row Count:977 --> [DB Rows: 25,285]
Highlighted Clustered Row Count: 977 --> [DB Rows:

Expression Builder: Not Assigned

Start Time: 01-01-90 00:00:

01/01/1990 00:00:00 - 1

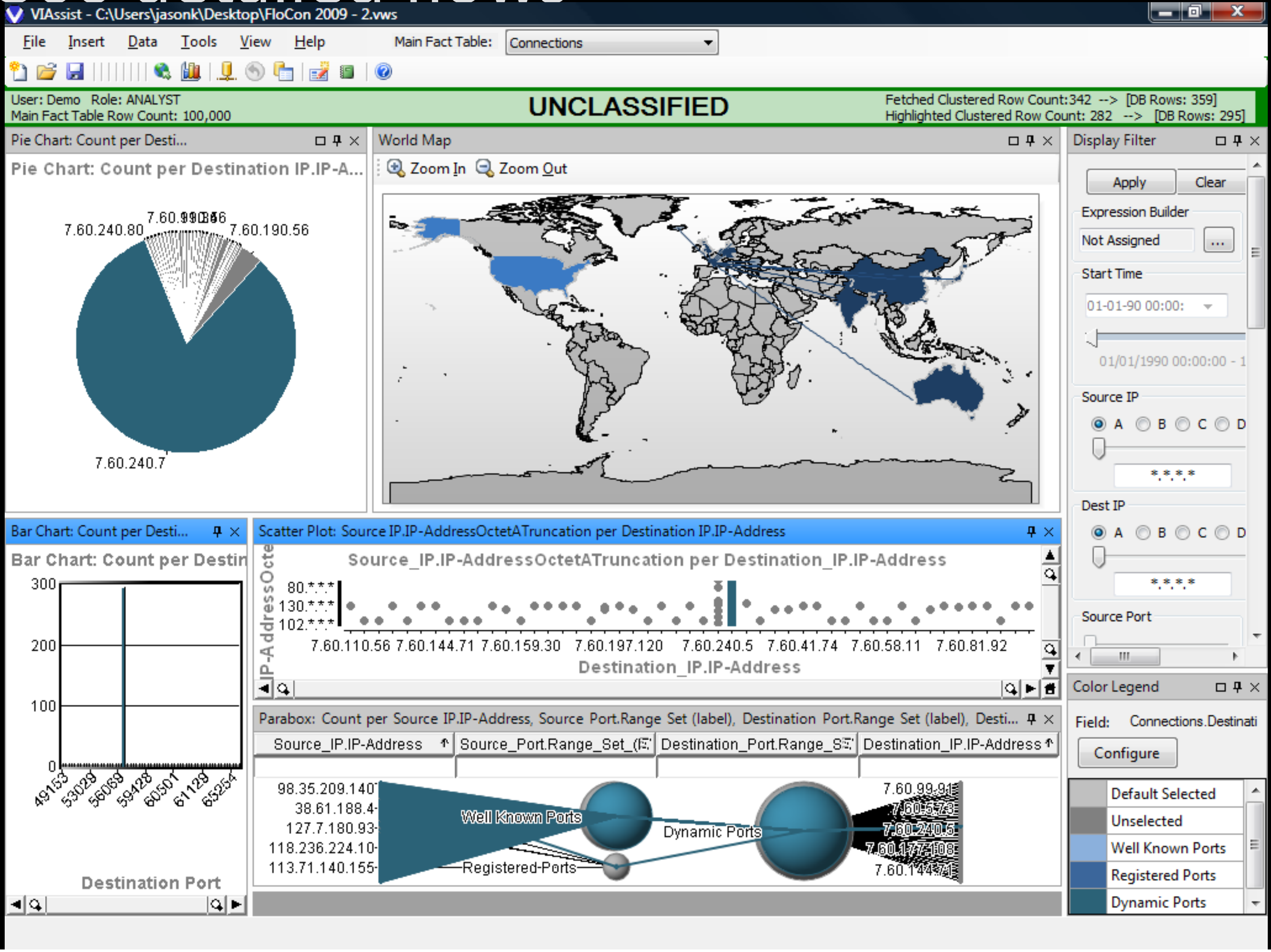
Source IP: ● A ○ B ○ C ○ D

Dest IP: ● A ○ B ○ C ○ D

Field: Connections.Destinati

Color Legend
Default Selected
Unselected
Well Known Ports
Registered Ports
Dynamic Ports

300 detailed flows



VIAssist - C:\Users\jasonk\Desktop\FloCon 2009 - 2.vws

Main Fact Table: Connections

User: Demo Role: ANALYST
Main Fact Table Row Count: 100,000

UNCLASSIFIED

Fetched Clustered Row Count:342 --> [DB Rows: 359]
Highlighted Clustered Row Count: 282 --> [DB Rows: 295]

Pie Chart: Count per Destination IP.IP-A...

World Map

Display Filter

Expression Builder: Not Assigned

Start Time: 01-01-90 00:00:

01/01/1990 00:00:00 - 1

Source IP: ● A ○ B ○ C ○ D — *.*.*.*

Dest IP: ● A ○ B ○ C ○ D — *.*.*.*

Source Port

Bar Chart: Count per Destin

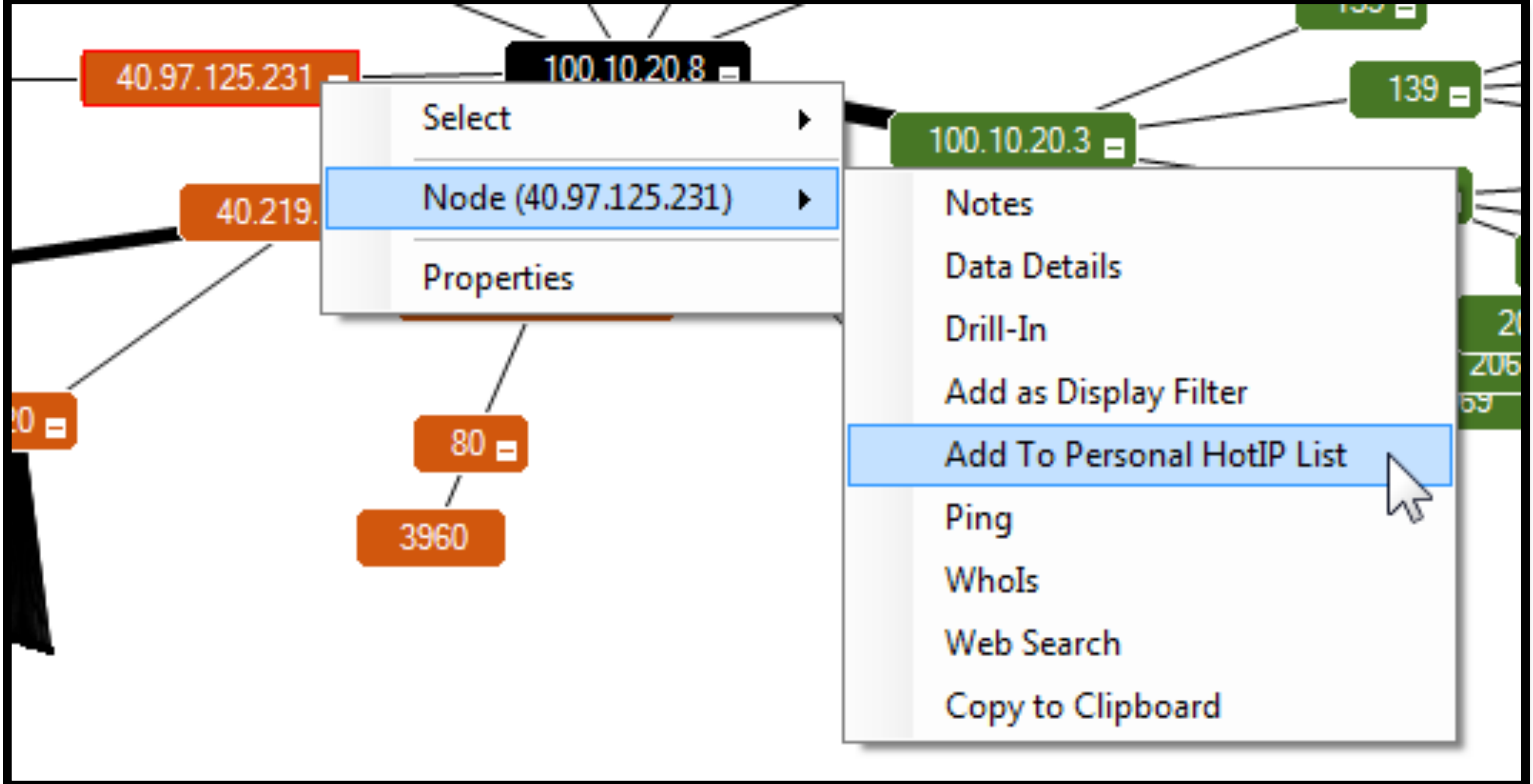
Scatter Plot: Source IP.IP-AddressOctetATruncation per Destination IP.IP-Address

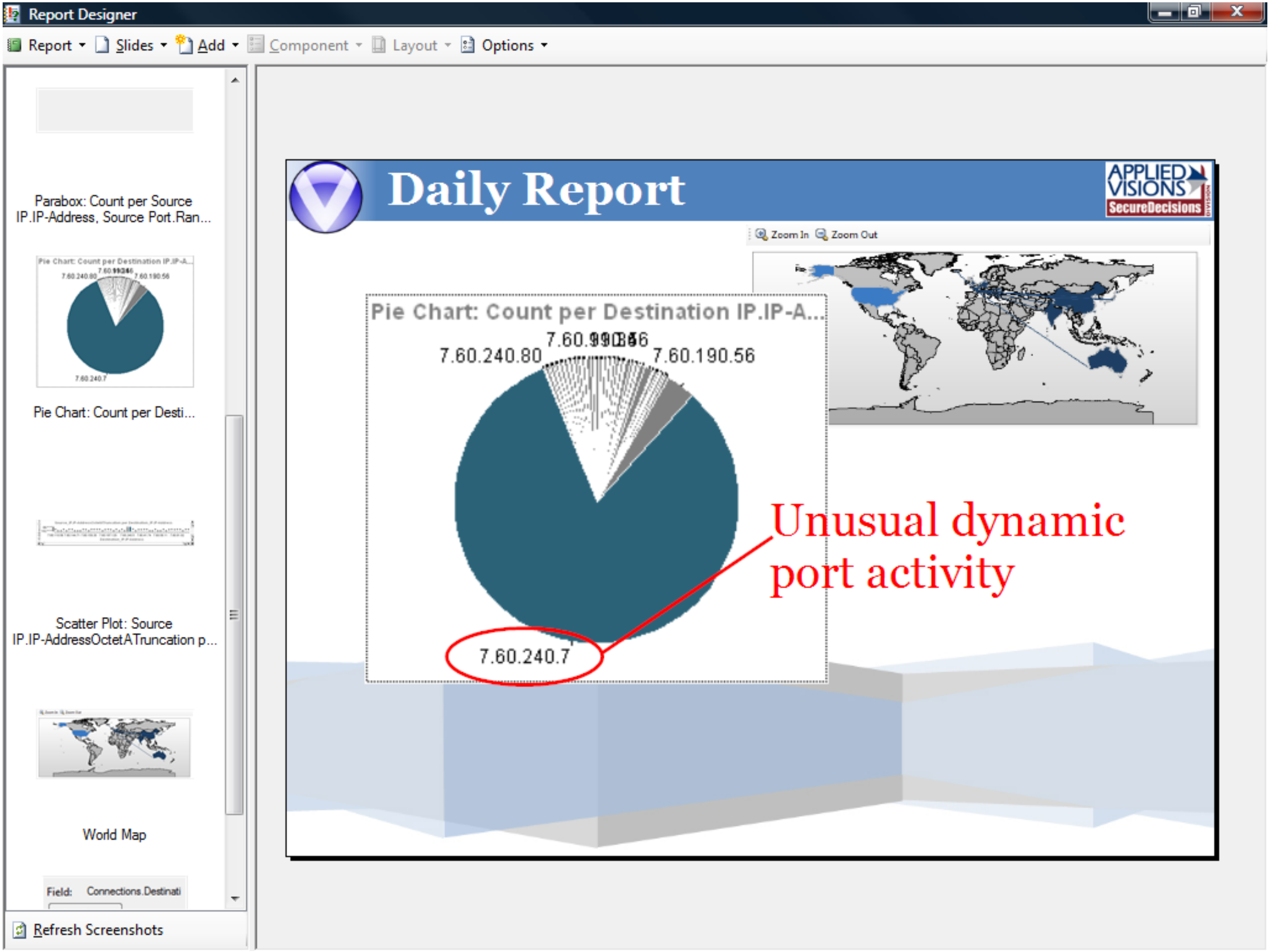
Parabox: Count per Source IP.IP-Address, Source Port.Range Set (label), Destination Port.Range Set (label), Desti...

Color Legend

Field: Connections.Destinati

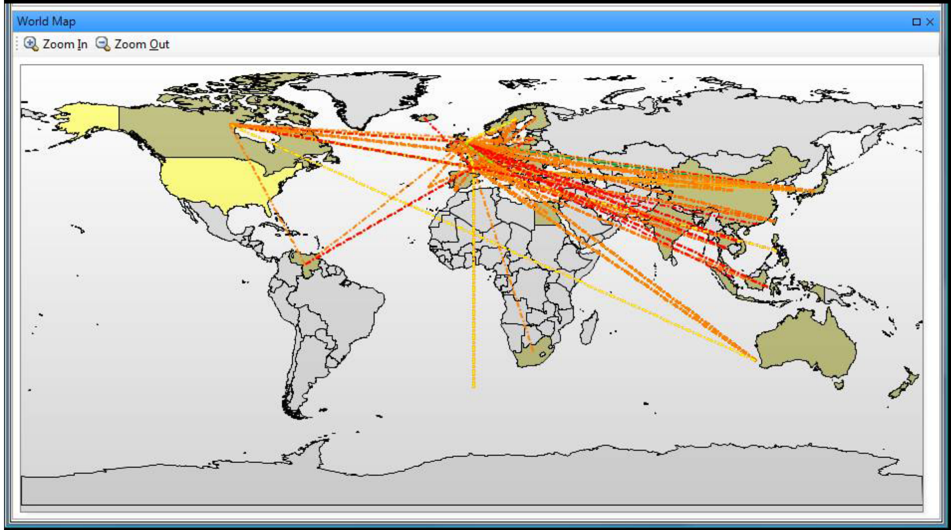
▢	Default Selected
▢	Unselected
▢	Well Known Ports
▢	Registered Ports
▢	Dynamic Ports

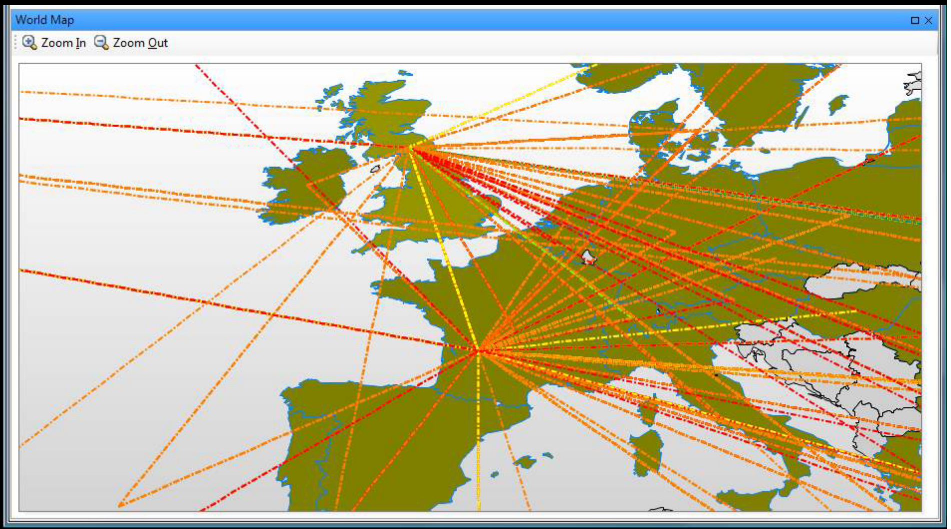

40.97.125.231
100.10.20.8
100.10.20.3
139
40.219.
80
3960
Select
Node (40.97.125.231)
Properties
Notes
Data Details
Drill-In
Add as Display Filter
Add To Personal HotIP List
Ping
WhoIs
Web Search
Copy to Clipboard

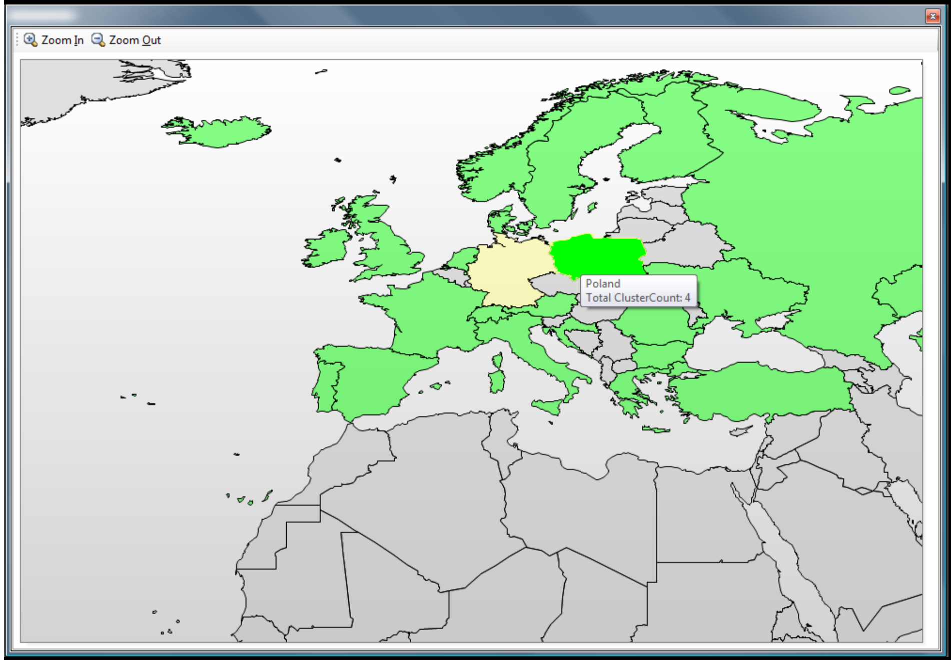

Report Designer
Report
Slides
Add
Component
Layout
Options
Parabox: Count per Source IP.IP-Address, Source Port.Ran...
Pie Chart: Count per Desti...
Scatter Plot: Source IP.IP-AddressOctetATruncation p...
World Map
Field: Connections.Destinati
Refresh Screenshots
APPLIED VISIONS
SecureDecisions
Zoom In
Zoom Out
Pie Chart: Count per Destination IP.IP-A...
7.60.240.80
7.60.99.186
7.60.190.56
7.60.240.7

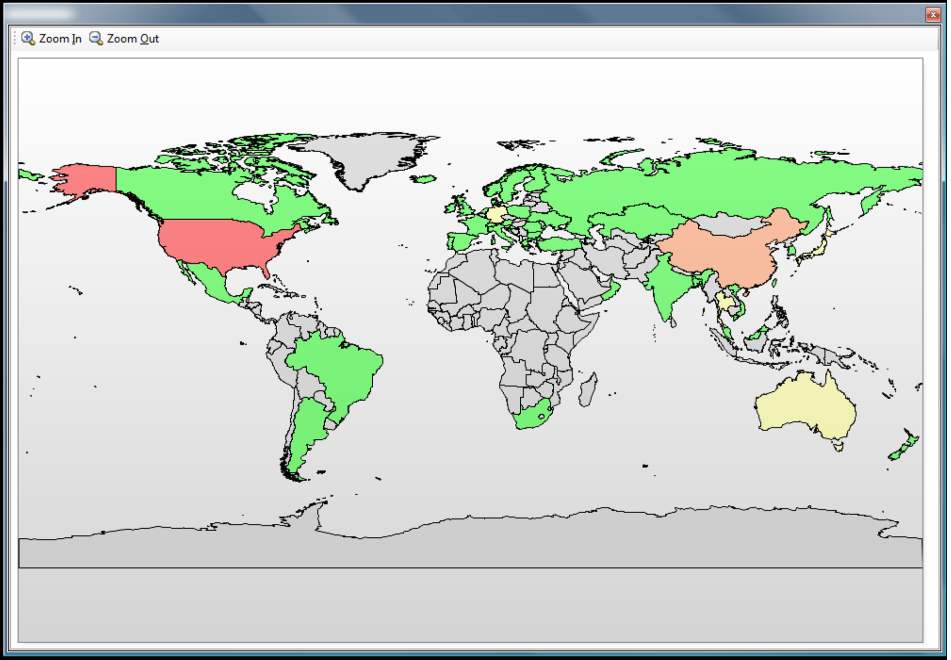
Daily Report

Unusual dynamic port activity

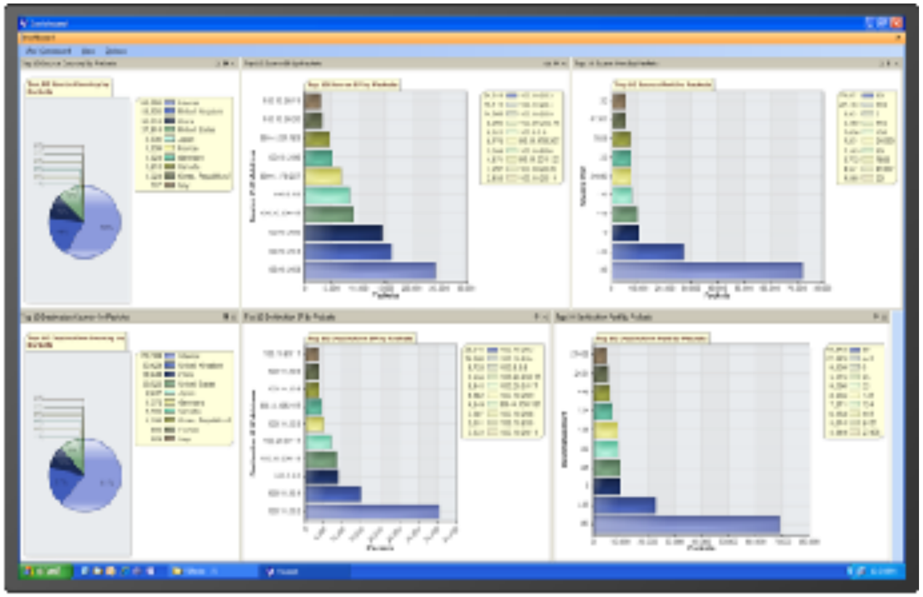

World Map
Zoom In
Zoom Out


World Map
Zoom In
Zoom Out


Zoom In
Zoom Out
Poland
Total ClusterCount: 4


Zoom In
Zoom Out

UNCLASSIFIED



Dr. John Goodall, johng@avi.com
Jason Kopylec, jasonk@avi.com

http://www.securedecisions.com/viassist