

# A Framework for Effective Alert Visualization

Uday Banerjee

Jon Ramsey

*SecureWorks*

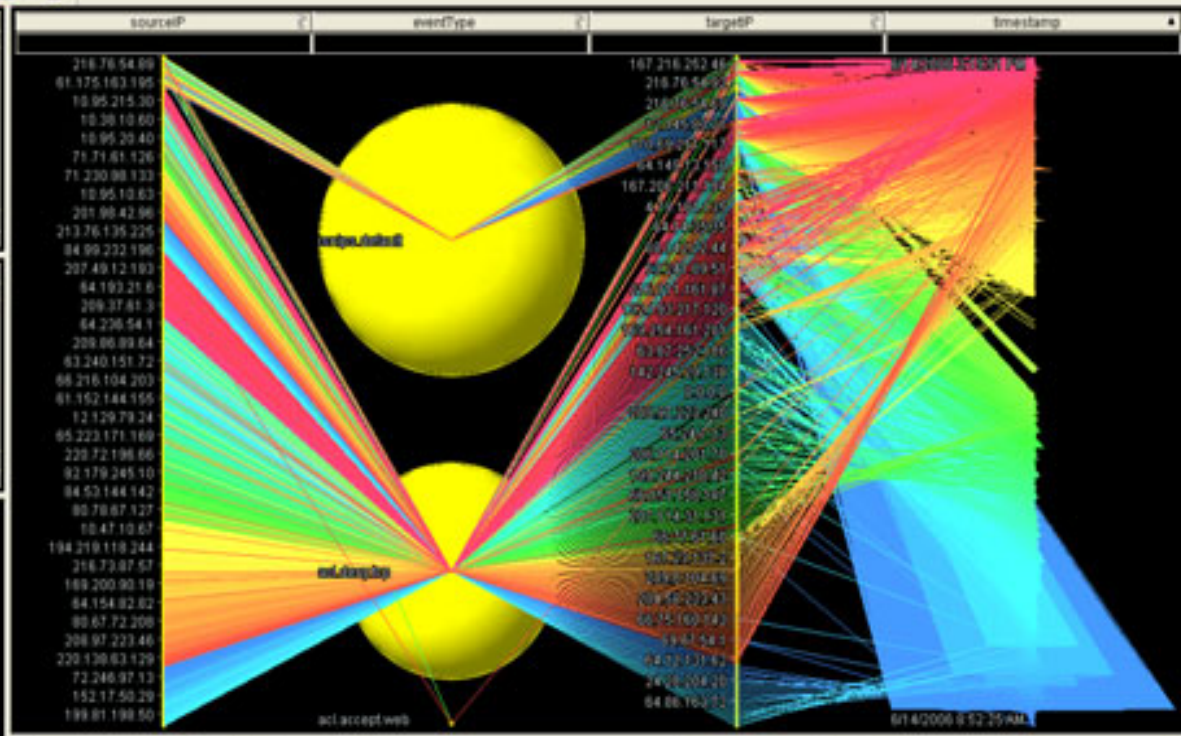
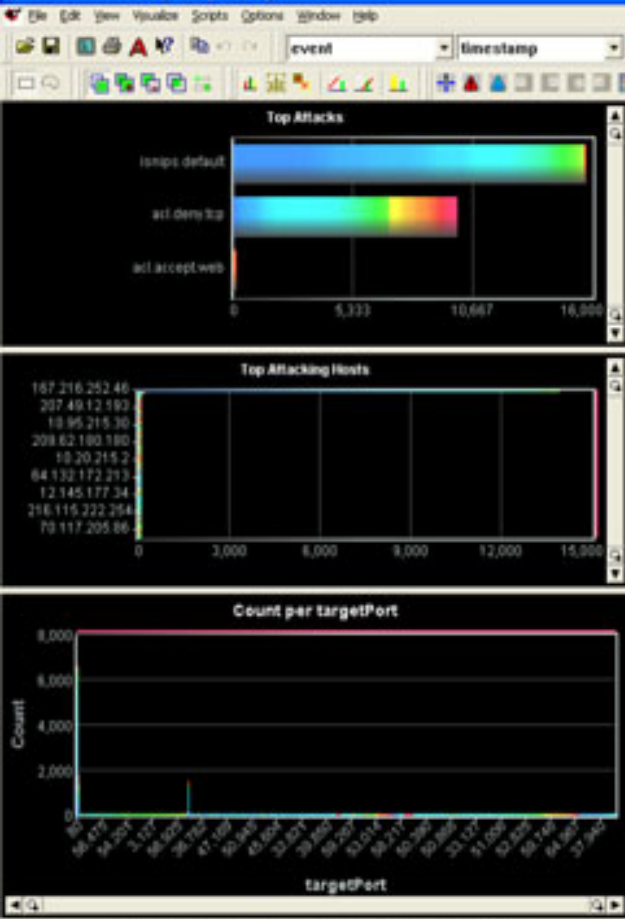
# Visualization

- Visualization has always been used – but mostly from a reporting standpoint
- We need to start pushing it from the Reporting space to the Analytical space

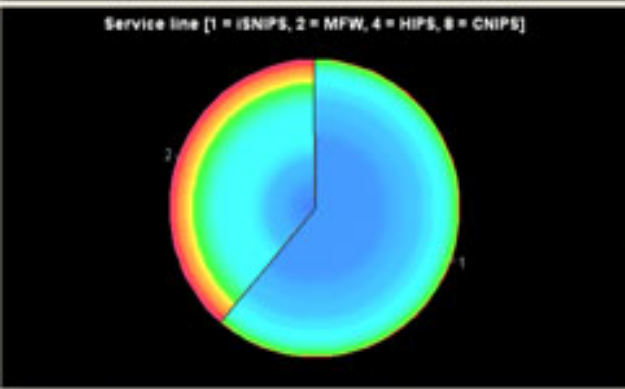
# Visualization

- Security departments/organizations deal with hundreds of thousands to millions(+) security alerts/messages a day from various devices:
  - IPS/IDS
  - Firewalls
  - AntiSpam / Antivirus devices, etc.
- Correlation is only so effective...
- Humans need to look at the outputs of the correlations, and should also be able to look at the larger picture to effectively analyze the situation





agent	event type	event	obj	prio.	sourceIP	targetIP
FNB SouthEast Operations	snips default	0006 ScriptWizdo Test Smae	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	8010 Email Attachment Time via SMTP	<NULL>	30	69.93.187.90	12.145.83.20
FNB SouthEast Operations	snips default	4871 SWZT7 Possible read view extensio	<NULL>	30	69.93.187.90	12.145.83.20
FNB SouthEast Operations	snips default	8010 Email Attachment Time via SMTP	<NULL>	30	201.217.120.254	12.145.83.20
FNB SouthEast Operations	snips default	0010 Email Attachment Time via SMTP	<NULL>	30	201.217.120.254	12.145.83.20
FNB SouthEast Operations	snips default	13779 SoapPoolP board4 SMTP	<NULL>	30	201.217.120.254	12.145.83.20
FNB SouthEast Operations	snips default	4871 SWZT7 Possible read view extensio	<NULL>	30	201.217.120.254	12.145.83.20
FNB SouthEast Operations	snips default	6435 VID11383 MSSQL_Serve Dataserv Over	<NULL>	30	222.216.222.9	12.145.83.20
FNB SouthEast Operations	snips default	17958 VID11383 MSSQL_Serve Dataserv Over	<NULL>	30	222.216.222.9	12.145.83.20
FNB SouthEast Operations	snips default	0006 ScriptWizdo Test Smae	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1
FNB SouthEast Operations	snips default	3616 SOC Test post 9999 to 2W	<NULL>	30	12.145.83.39	63.239.86.1



# The case for Visualization

- Visualization is a very effective way to represent large volumes of information in a succinct manner
- Allows one to look at the same data from multiple viewpoints
- Allows one to look “around” the alerts that you are investigating to gain some additional perspective

# What makes a good visualization?

- Data driven display: we should be able to 'slice and dice' the data, bring related events into focus based on the data selected. E.g. select data by:
  - Protocol
  - IP Address
  - Timestamp
  - Asset Value
  - PortAnd have it bring into focus all related alerts.
- Multiple views into the same data: can elicit a different perspective

# What makes a good visualization? (contd.)

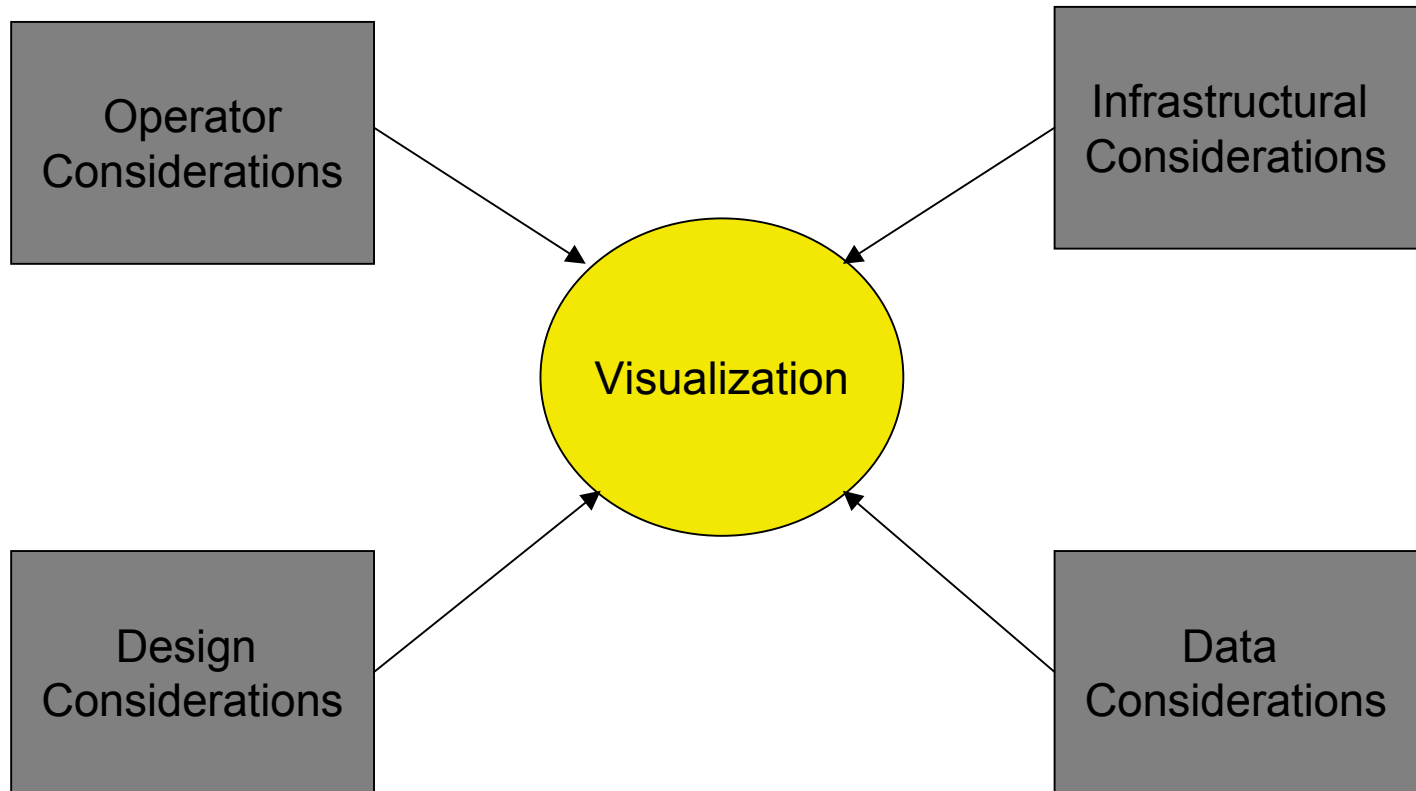
- Data linkage across all views
- On-the-fly customization of views
- Drill down/Zoom out : allows to isolate a particular event-set or allows you to see the big picture
- Data suppression : allows to quickly eliminate data that is of no consequence to the analysis (e.g. UDP traffic when analyzing TCP flows)
- Statistical information : It is useful to know information on total or selected events (like totals, maximum values, unique values, etc.) to gain a perspective on the nature of the activity



# What makes a good visualization? (contd.)

- Other desirable features:
  - Realtime visualizations
  - Interoperability with other systems (ticketing, reporting)
  - Easily accessible (via a web browser?)

# Considerations for Effective Visualization



# Data Considerations

- Richer data sets make for better visualizations. We need to gather as much information around the event as possible
- Data should be normalized
- More visual correlation can be performed if there are a large number of data fields to work with. Some examples:
  - Device Interface > Tells you which interface the IDS/IPS alert was detected on > Tells us if the alert traffic was inbound or outbound
  - Action taken > was this alert blocked or allowed? > Different responses to alerts from IPS versus IDS
  - IP addresses > is the source IP on our 'attacker' watchlist?
  - Type of signatures tripped > specific attack or general scan

# Infrastructural considerations

- Dedicated, capable database used exclusively for storing visualization data (allows for the flexibility to add/remove/modify content without affecting other production systems)
- Visualization tools should have access to other databases like Asset and Vulnerability databases so they can provide even more context

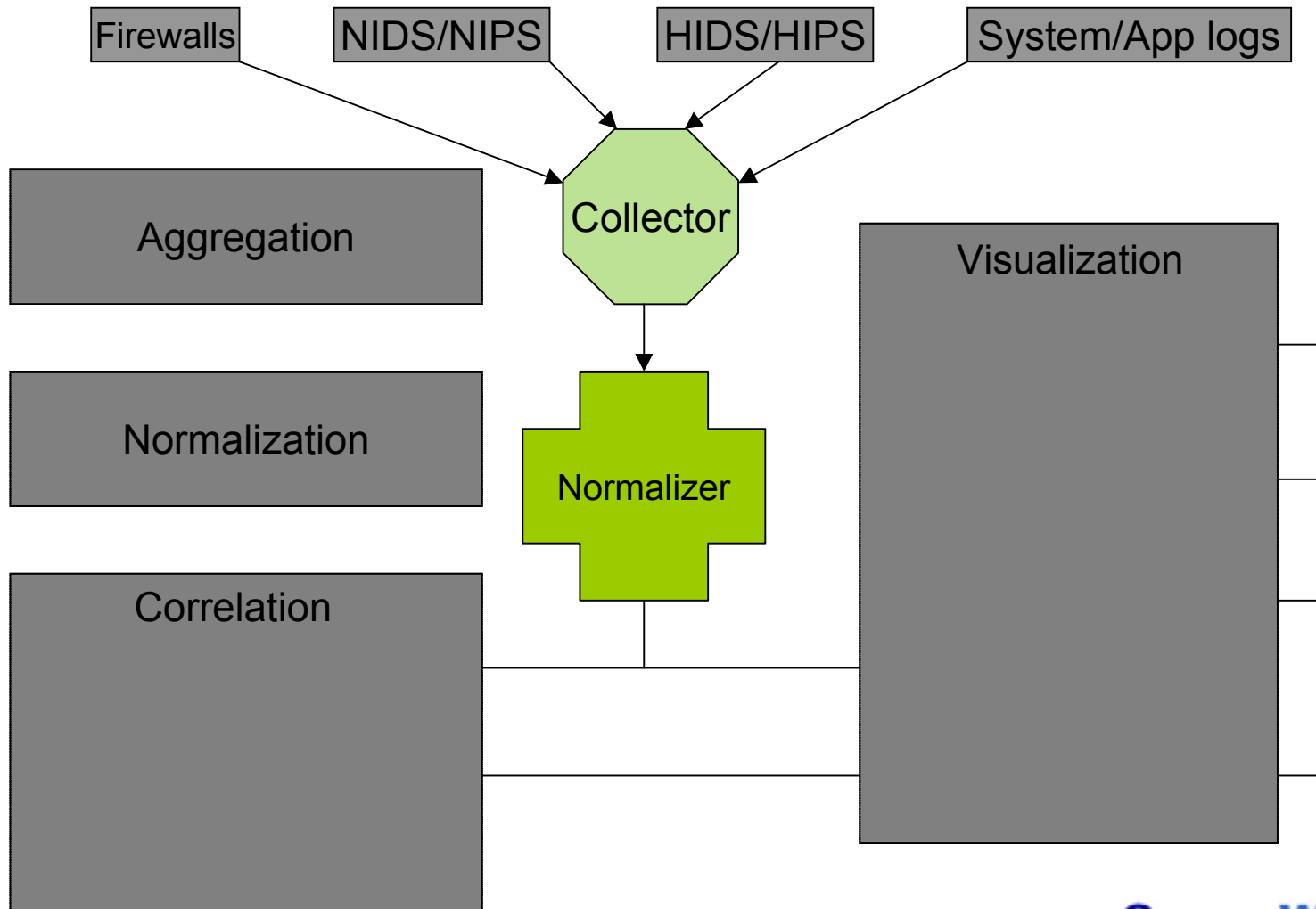
# Operator Considerations

- If using color to key off on events, the ability of the operator to discern colors must be taken into consideration
- Screen real estate is *\*very\** important
- Training
  - Using data from real scenarios

# Design Considerations

- Design of the visualization is of utmost importance (layout, intuitiveness, features)
- The visualizations should be presented in such a way that inferences should quite literally, present themselves

# Data Flow through the system

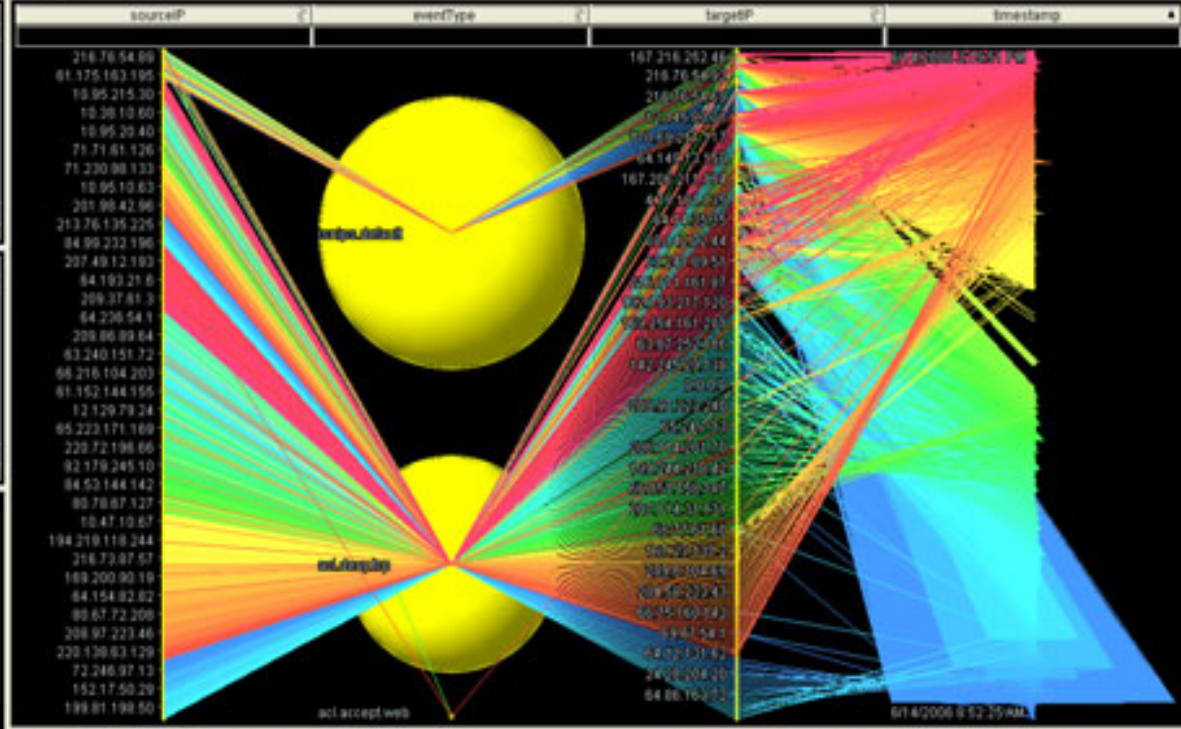
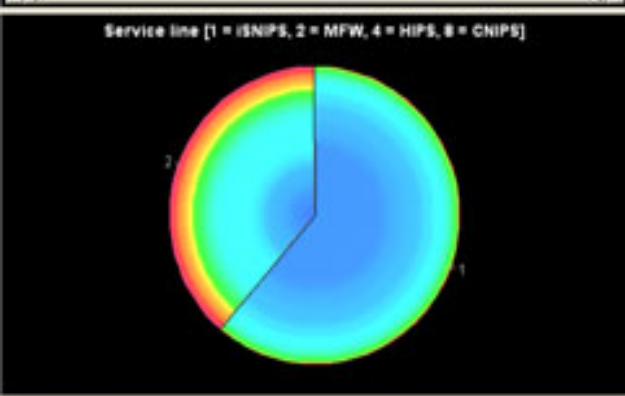
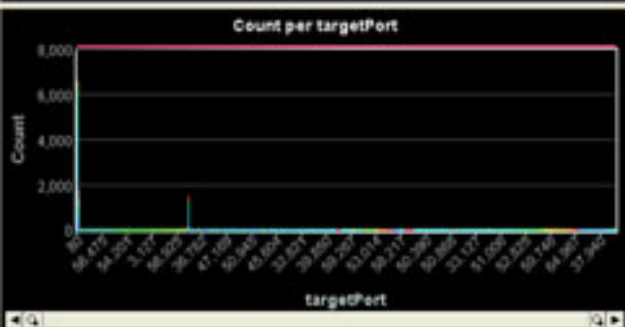
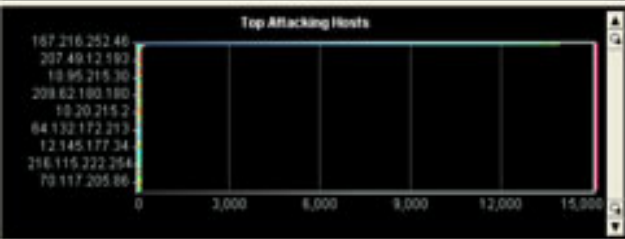
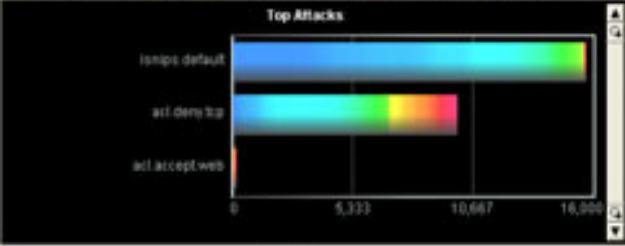


# Integration with our SIM Tool

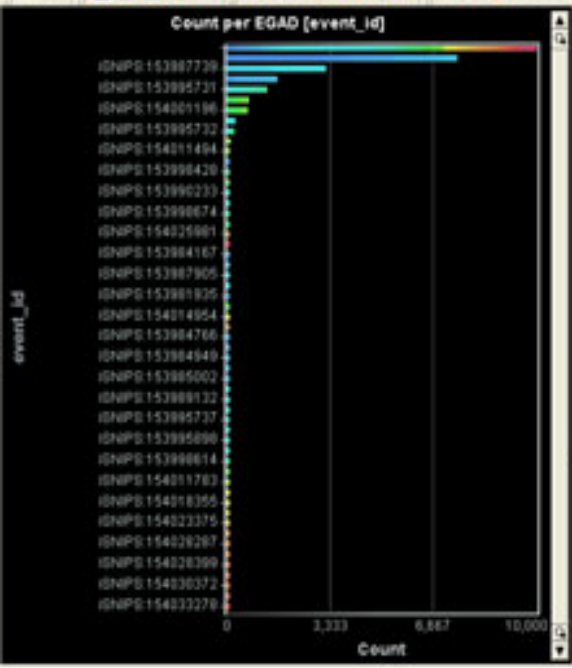
The screenshot displays the SecureWorks SIM Tool interface. The main window shows a list of events with columns for Obs, Events, SVC Line, Highest Sev. Obs, Sev, Company Name, % Age, and Owner. A context menu is open over one of the rows, showing options like 'Launch Gibraltar', 'Launch All', 'Release Ownership', 'Physical Ticket', 'SendView @Risk', 'Preferences', 'Refresh', 'Select All', 'Print', 'Export', 'Copy', and 'Help'.

Obs	Events	SVC Line	Highest Sev. Obs	Sev	Company Name	% Age	Owner
5	55	0000%	temp.default	75	Arnold Golden Gregory	8431 m	sgmwrk
8	35	0000%	temp.default	75	Banking Savings Bank	8430 m	
35	1505	0000%	temp.default	80	Hopkint Federal Credit Union	8430 m	
4	278	0000%	temp.default	75	Bank First Staff Federal Credit Union	8430 m	
2	13	0000%	temp.default	75	Gloves Community Hosp Assoc	8429 m	
1	7	0000%	temp.default	75	Northwest Bank	8429 m	
8	82	0000%	info.us.high	75	ECG Technologies	8429 m	
15	375	0000%	info.us.high	75	Tilly Bank	8424 m	
36	264	0000%	temp.default	75	Hilbing Cooper State Credit Un	8422 m	
49	1141	Multiple	temp.default	75	Address Avenue Federal Credit Union	8421 m	
2	8	0000%	temp.default	75	Liberty First Credit Union	8414 m	
1	8	0000%	temp.default	75	MCN Personnel Management	8413 m	
3	48	0000%	temp.default	75	Congressional Federal Credit Union	8412 m	
4	25	0000%	temp.default	75	South Florida Educational Union of Credit	8411 m	
1	2	0000%	temp.default	75	The Foundation Trust Companies	8411 m	
8	13	0000%	temp.default	75	US Senate Federal Credit		
2	278	0000%	temp.default	75	Coast Bank for Savings		sgmwrk
1	18	0000%	temp.default	75	United Suburbs		
11	214	0000%	temp.default	75	Blue Ridge EMC		
26	332	0000%	temp.default	75	Wescom Credit Un		
4	85	0000%	temp.default	75	NASA Federal Credit Un		
8	98	0000%	temp.default	75	Gloves Bank Merit		
1	8	0000%	temp.default	75	Springdale Credit Un		
1	188	0000%	temp.default	75	Northwest Federal Credit		
1	27	0000%	temp.default	75	Teachers Credit Un		
1	18	0000%	temp.default	75	All Accounting FCI		
18	31	0000%	temp.default	75	North Carolina Secretary		
28	11741	Multiple	temp.default	75	FBI Southern		
1	8	0000%	temp.default	75	Spanders FCI		
1	2	0000%	temp.default	75	Standard Bank Par		
1	5	0000%	temp.default	75	Flag Credit Union		
2	38	0000%	temp.default	75	Walworth Valley Power As		
8	81	0000%	temp.default	75	Clearview FCI	8388 m	
5	45	0000%	temp.default	75	Wiking Bank	8384 m	
1	1	0000%	temp.default	75	Lebanon Federal Credit Union	8382 m	
8	29	0000%	temp.default	75	Consolidated Electric Co. op	8381 m	
26	854	0000%	temp.default	75	Northway Bank	8379 m	
14	302	0000%	temp.default	75	Prosper Bank	8378 m	
8	82	0000%	temp.default	75	First National Bank of Savannah	8378 m	
2	48	0000%	temp.default	75	East Coast of Georgia	8378 m	
5	358	Multiple	temp.default	75	Clawson Federal Credit Union	8374 m	
7	81	0000%	temp.default	75	Indiana University CO	8373 m	
7	148	0000%	temp.default	75	1_Sun-Corporation	8370 m	
1	28	0000%	temp.default	75	MBFinancial	8369 m	
18	471	Multiple	temp.default	80	Michigan State Federal Credit Union	8365 m	
2	26	0000%	temp.default	75	West Bend Savings Bank	8363 m	
12	388	Multiple	info.us.high	75	Barclays	8361 m	
2	43	0000%	temp.default	75	Members First Credit Union of New Hampshire	8360 m	
18	798	0000%	temp.default	75	White Sands Credit Union	8359 m	
37	738	0000%	temp.default	75	W. Joseph Healthcare	8359 m	
3	42	0000%	temp.default	75	Gainesville Bank & Trust	8359 m	
3	8	0000%	temp.default	75	Graves Federal Savings and Loan Associa	8358 m	
1	5	0000%	temp.default	75	MPay Inc Software	8356 m	
1	152	0000%	info.us.high	75	Windsor Island Credit Union	8354 m	
8	128	0000%	temp.default	75	Peo. Nat. Feder of Credit Union	8349 m	
2	18	0000%	temp.default	75	Paragon FCI	8349 m	
18	2582	0000%	temp.default	75	American National Bank of Texas	8348 m	
5	878	0000%	temp.default	75	First Bank & Trust	8343 m	
1	1	0000%	temp.default	75	The Methodist Central Credit Society	8342 m	

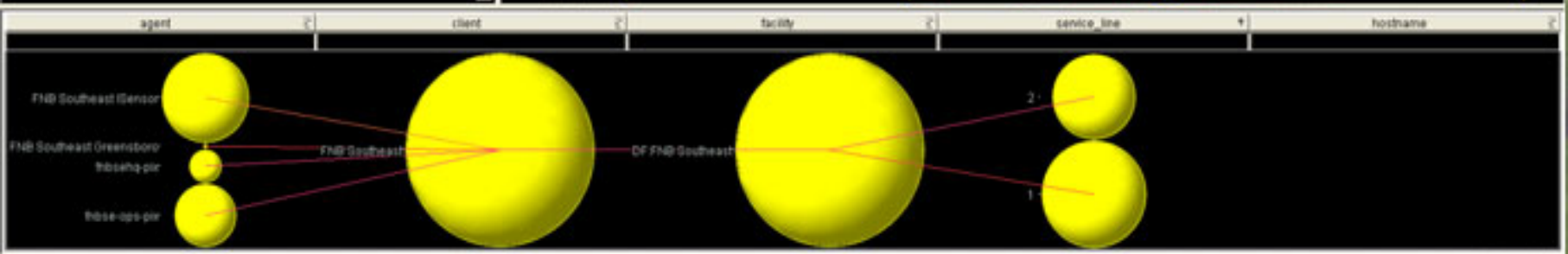
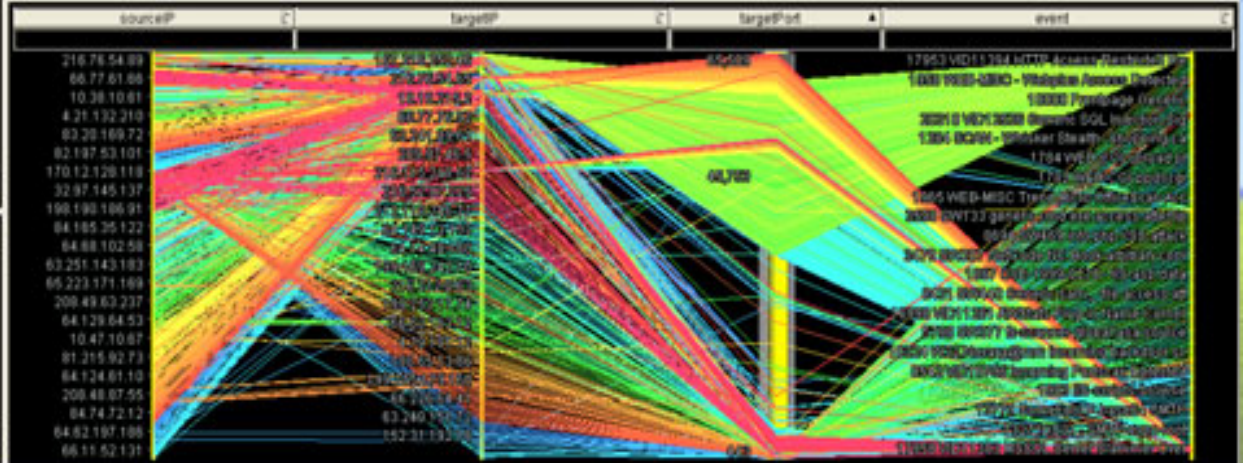
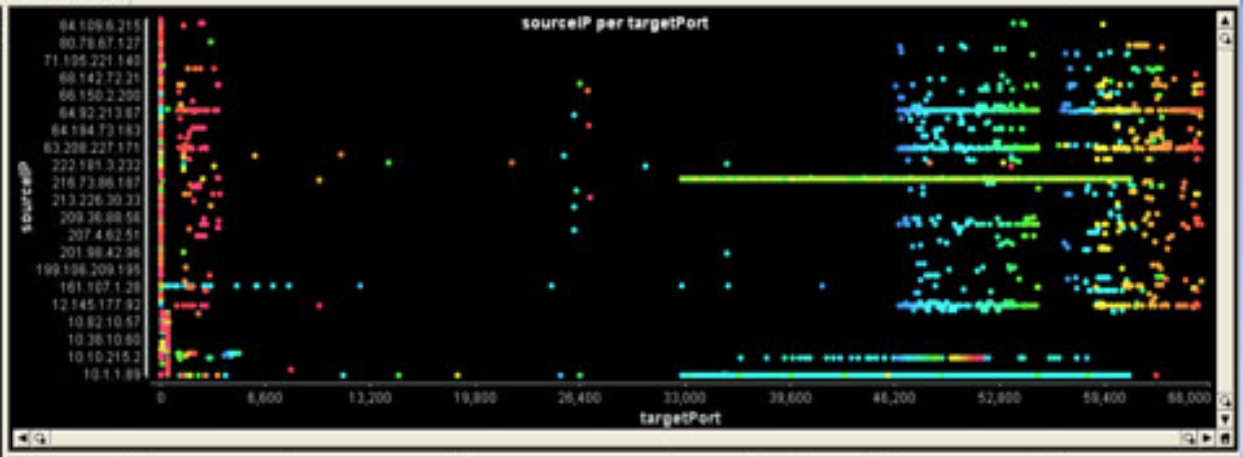


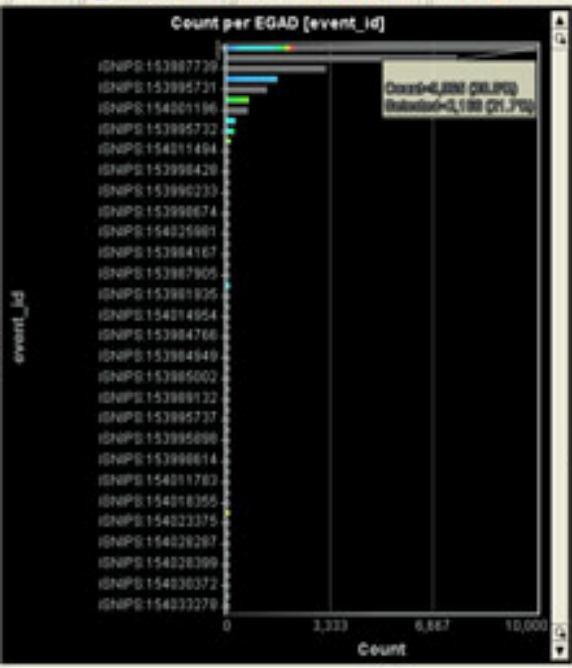


agent	eventType	event	obj	prio	sourceIP	targetIP
FNB_SoftSwat_Overshoo	snipe.default	0006 ScriptWizdo Test Snare	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	8010 Email Attachment Time via SMTP	<NULL>	30	69.93.187.90	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	4871 SWZ77 Possible read_virus_extensi	<NULL>	30	69.93.187.90	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	8010 Email Attachment Time via SMTP	<NULL>	30	201.217.120.254	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	0010 Email Attachment Time via SMTP	<NULL>	30	201.217.120.254	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	13779 SoapPoolP board4 SMTP	<NULL>	30	201.217.120.254	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	4871 SWZ77 Possible read_virus_extensi	<NULL>	30	201.217.120.254	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	6405 VID11383 MSSQL_Serve_Database_Ove	<NULL>	30	220.216.222.9	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	17958 VID11383 MSSQL_Serve_Database_Ove	<NULL>	30	220.216.222.9	12.145.83.20
FNB_SoftSwat_Overshoo	snipe.default	0006 ScriptWizdo Test Snare	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1
FNB_SoftSwat_Overshoo	snipe.default	3616 SOC Test post 9999 to ZW	<NULL>	30	12.145.83.39	63.239.86.1

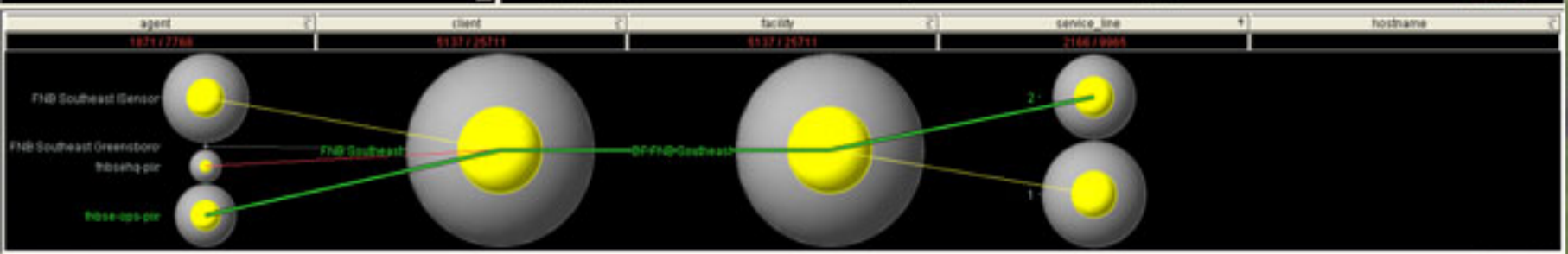
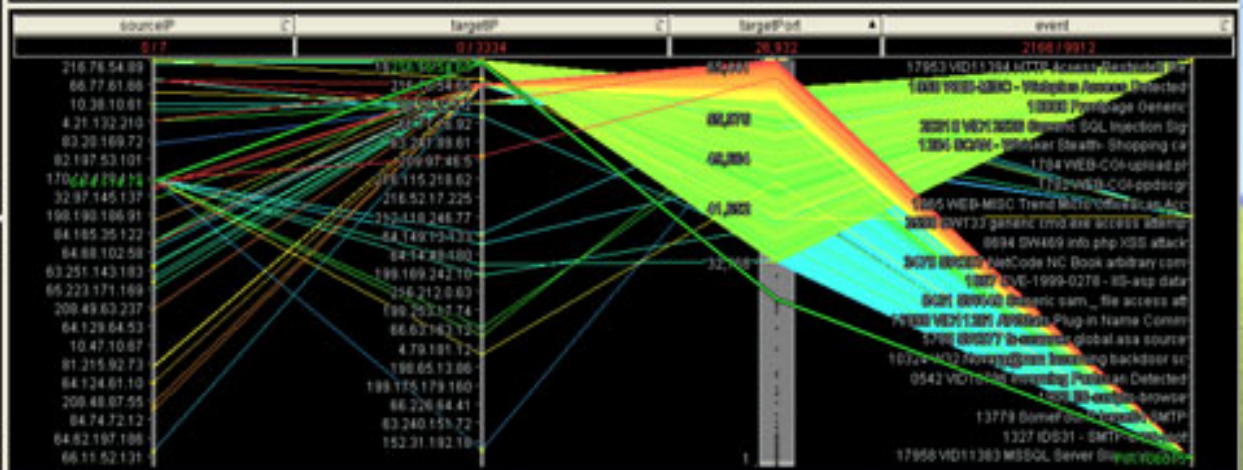
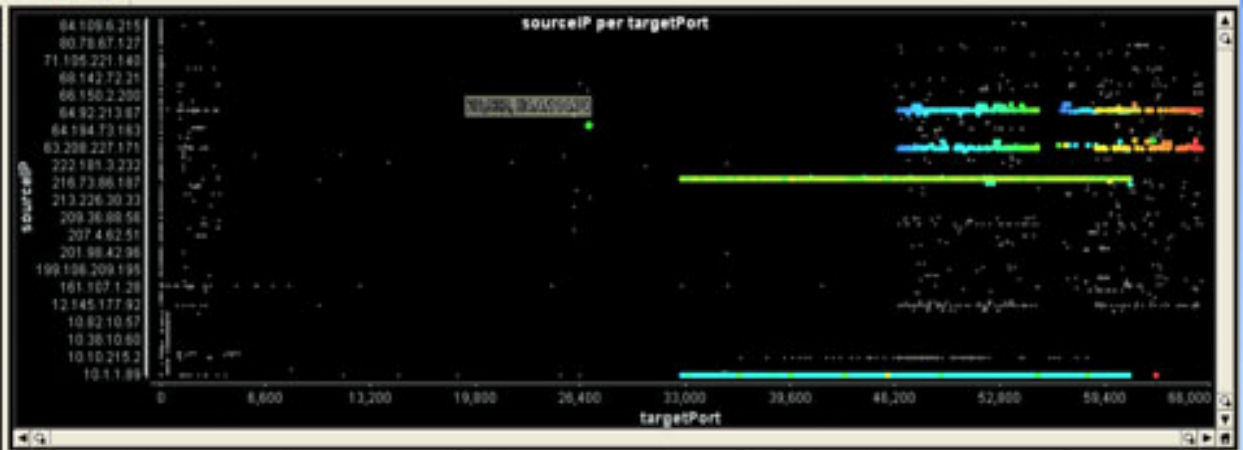


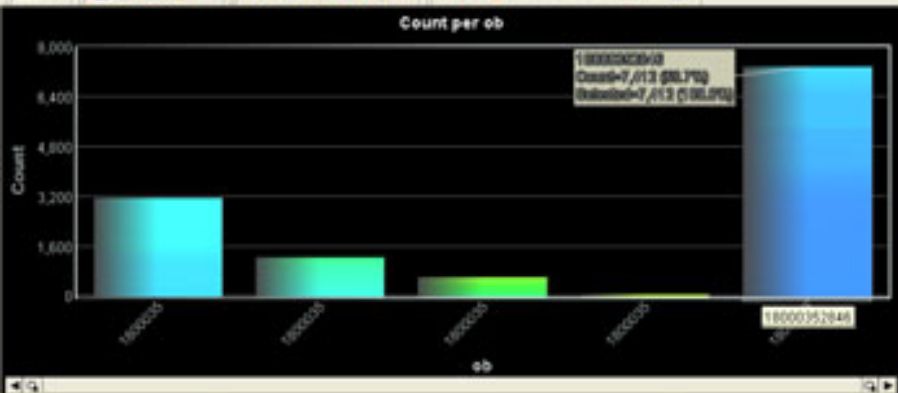
Statistic	comCount
Selected	Integer
Mean Sel	1
Max Sel	1
Min Sel	1





Statistic	comCount
Selected	Integer
Mean Sel	5,137
Max Sel	1
Min Sel	1
Max Sel	1





Details

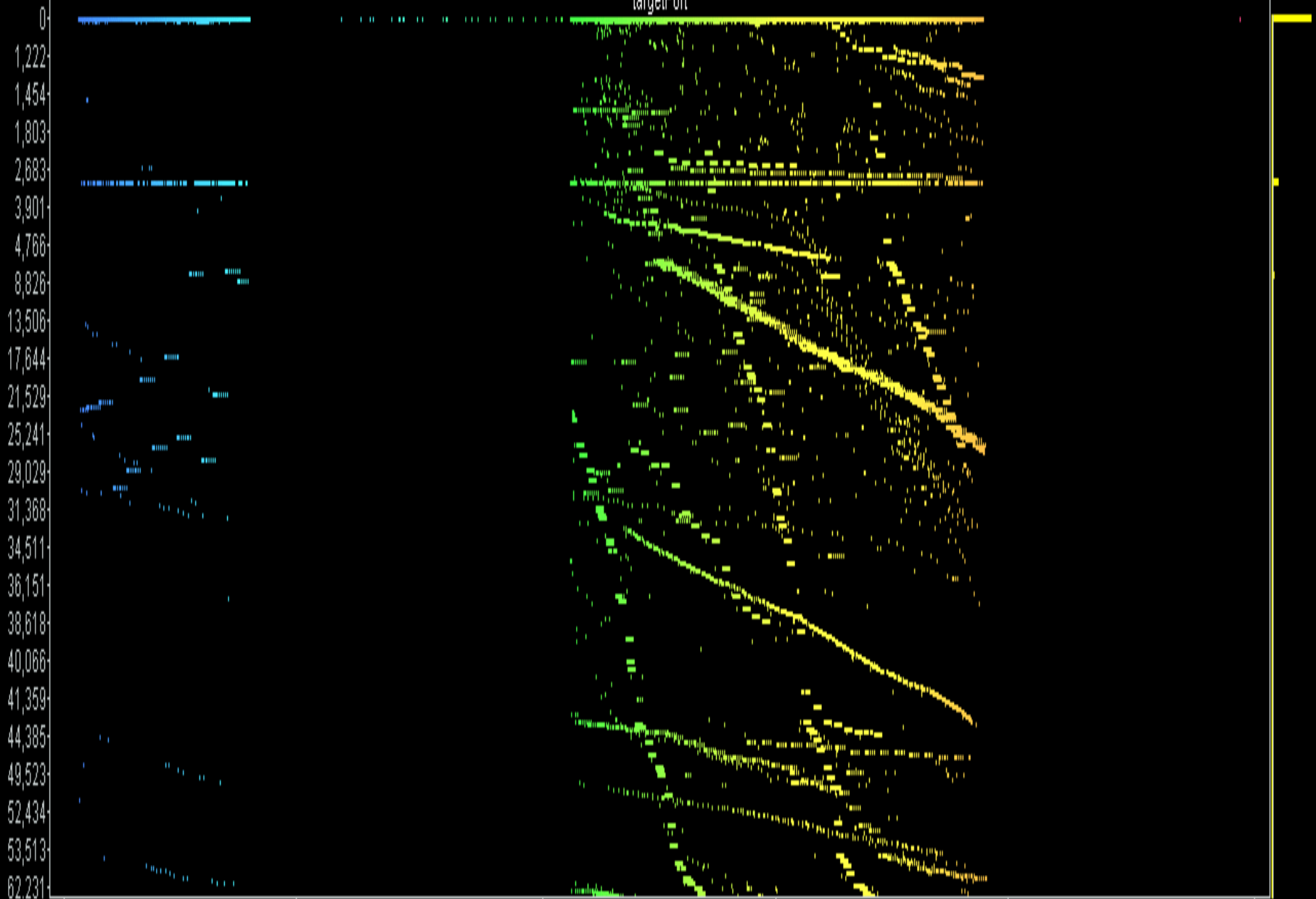
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>

action_taken	agent	client	event	eventType	ob	oe_ev_id	priority	proto	service_line	sourceIP	targetIP	targetPort	timestamp	t_ev_id
1	FNB Southeast Disease	FNB Southeast	1793 V1	usage defect	<NULL>	<NULL>	30	<NULL>		1 216.76.54.89	167.216.2...	45,390	6/14/2006 9:54:16 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	2037 V1	usage defect	18000353	<NULL>	50	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:54:42 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1793 V1	usage defect	<NULL>	<NULL>	50	<NULL>		1 216.76.54.89	167.216.2...	42,381	6/14/2006 9:55:21 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1993 W8	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:54:37 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1793 V1	usage defect	<NULL>	<NULL>	30	<NULL>		1 216.76.54.89	167.216.2...	51,410	6/14/2006 9:55:27 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1793 V1	usage defect	<NULL>	<NULL>	30	<NULL>		1 216.76.54.89	167.216.2...	46,792	6/14/2006 9:55:23 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1796 DG	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:54:14 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1796 DG	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:54:13 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1961 W8	usage defect	18000353	<NULL>	50	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:53:44 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1796 DG	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:55:51 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	2037 V1	usage defect	18000353	<NULL>	50	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:55:09 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	3830 SW	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:54:48 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1796 DG	usage defect	18000353	<NULL>	50	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:55:04 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1796 DG	usage defect	18000353	<NULL>	50	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:54:02 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	3830 SW	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:55:33 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1796 DG	usage defect	18000353	<NULL>	30	<NULL>		1 167.216.232	216.76.54...	80	6/14/2006 9:53:39 AM	<NULL>
1	FNB Southeast Disease	FNB Southeast	1793 V1	usage defect	<NULL>	<NULL>	30	<NULL>		1 216.76.54.89	167.216.2...	48,375	6/14/2006 9:55:22 AM	<NULL>

ev\_Details

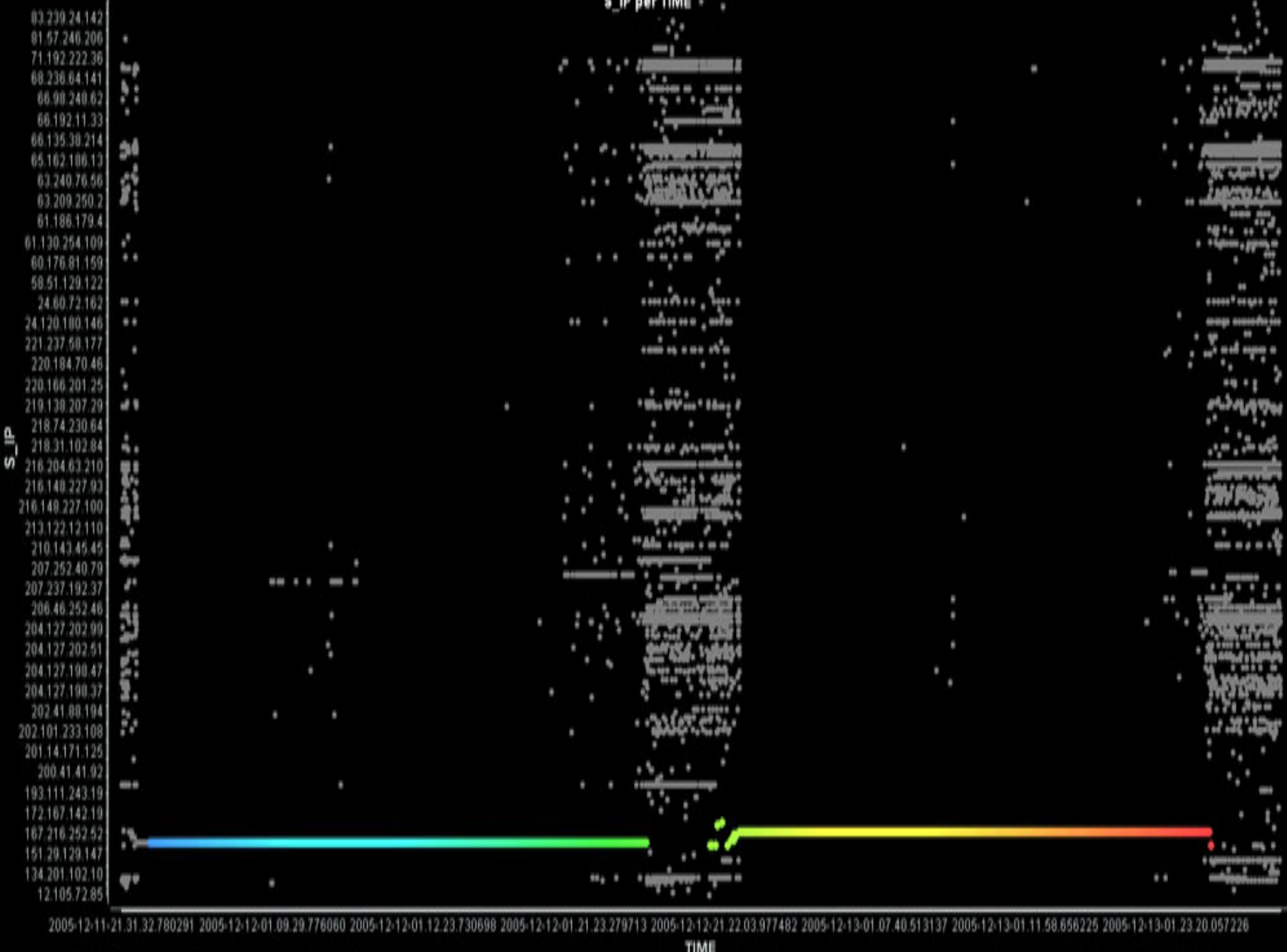
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>
<NULL>

targetPort



6/27/2006 11:45:00 PM 6/28/2006 3:45:00 AM 6/28/2006 8:00:00 AM 6/28/2006 12:00:00 PM 6/28/2006 4:00:00 PM 6/28/2006 8:15:00 PM

# S\_IP per TIME



# Visualization: caveats

- Only becomes more effective as data grows larger
- May not be very suitable for quickly analyzing very small amounts of data

# Some useful views

- Source IP vs Target IP vs Timestamp
- Source IP vs Target Port
- Source IP vs Alert Timestamp
- Dest Port vs Alert Timestamp
- Counts by (S\_IP, T\_IP, T\_Port, etc.)
- Attacks vs Asset value vs Vulnerabilities



# Demo

Questions?  
Comments?

[ubanerjee@secureworks.com](mailto:ubanerjee@secureworks.com)