# A Framework for Effective Alert Visualization

Uday Banerjee

Jon Ramsey

*SecureWorks*

SecureWorks
The Information Security Experts

# Visualization

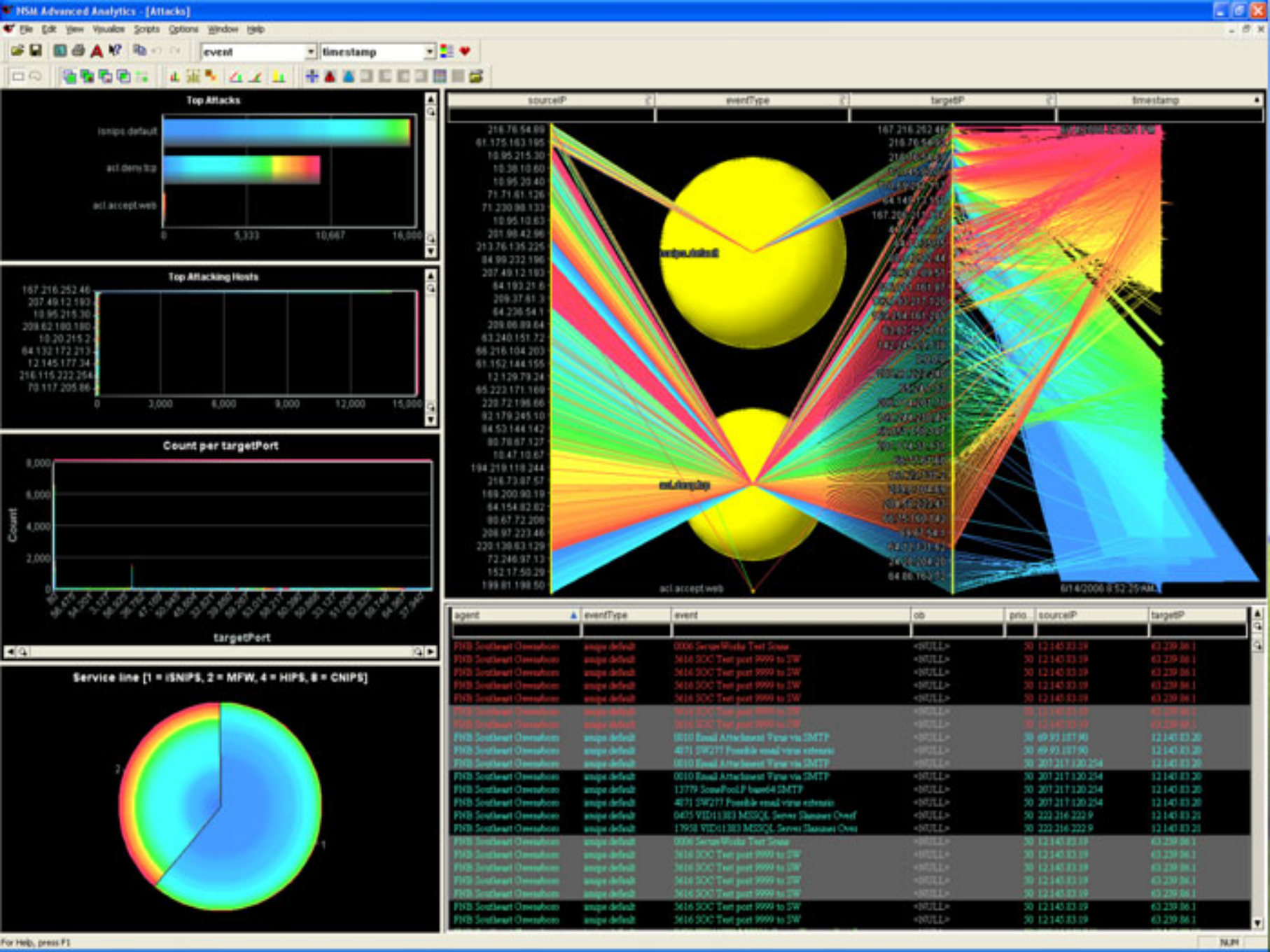
- Visualization has always been used – but mostly from a reporting standpoint
- We need to start pushing it from the Reporting space to the Analytical space

# 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

# Visualization (contd.)


SecureWorks
The Information Security Experts


MSM Advanced Analytics - [Attacks]
File Edit View Visualize Scripts Options Window Help
event
timestamp
Top Attacks
isnips default
acl.deny.tcp
acl.accept.web
0
5,333
10,667
16,000
Top Attacking Hosts
167.216.252.46
207.49.12.193
10.95.215.30
209.62.180.180
10.20.215.2
64.132.172.213
12.145.177.34
216.115.222.254
70.117.205.86
0
3,000
6,000
9,000
12,000
15,000
Count per targetPort
8,000
6,000
4,000
2,000
0
Count
targetPort
Service line [1 = iSNIPS, 2 = MFW, 4 = HIPS, 8 = CNIPS]
sourceIP
eventType
targetIP
timestamp
acl.accept.web
agent
eventType
event
ob
prio
sourceIP
targetIP
For Help, press F1
NUM

# 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
  - Port

  And have it bring into focus all related alerts.
- Multiple views into the same data: can elicit a different perspective

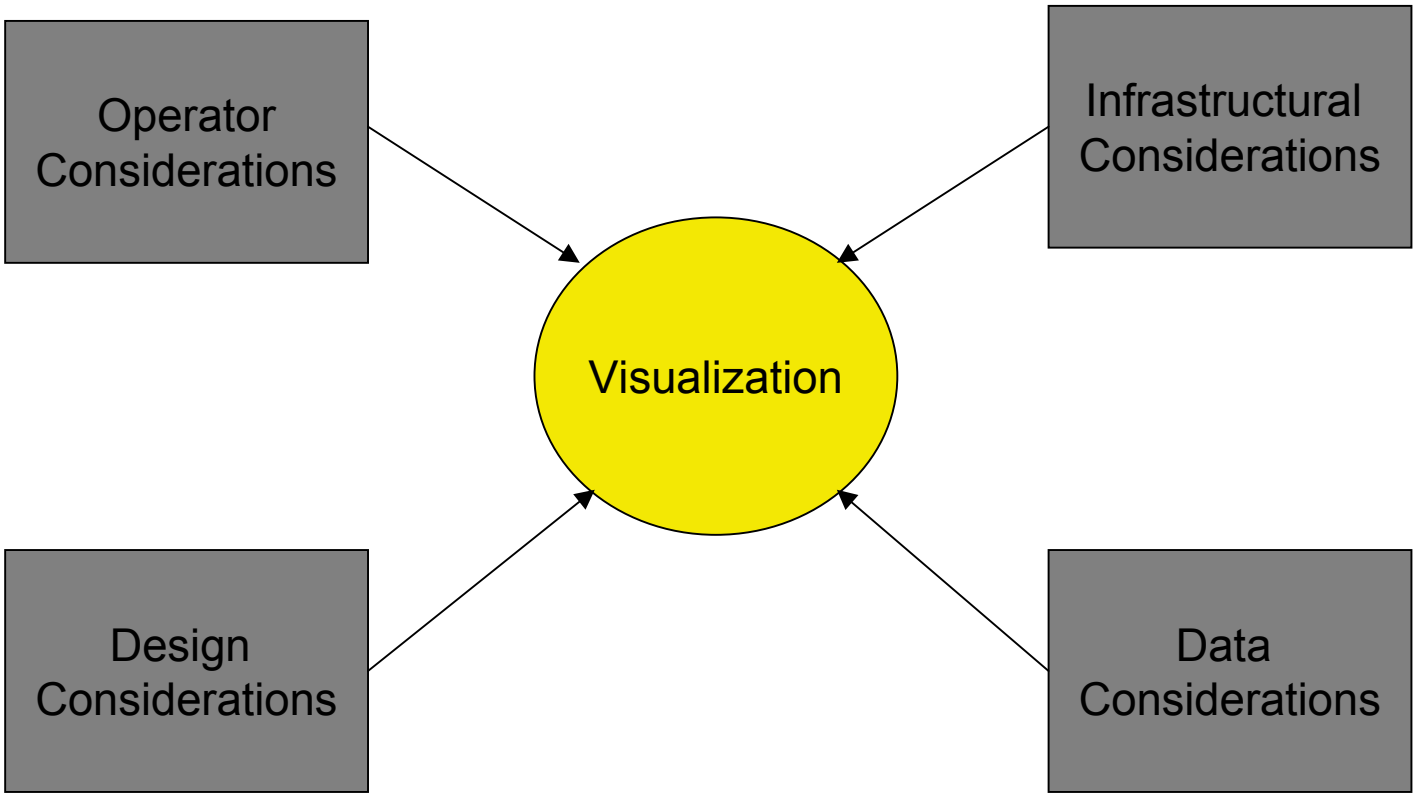
# What makes a good visualization? (contd.)

- 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

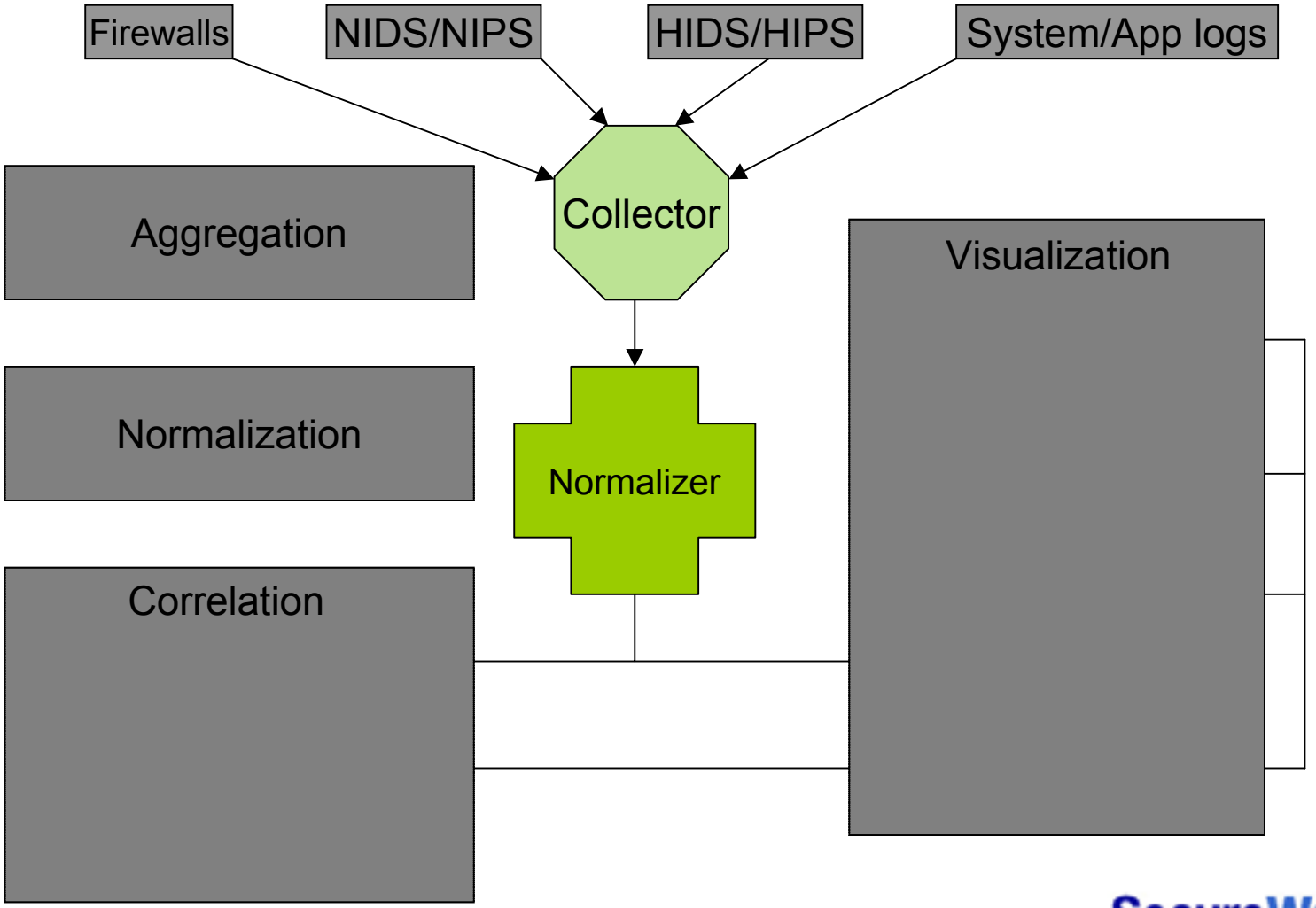
# Operator Considerations

- 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

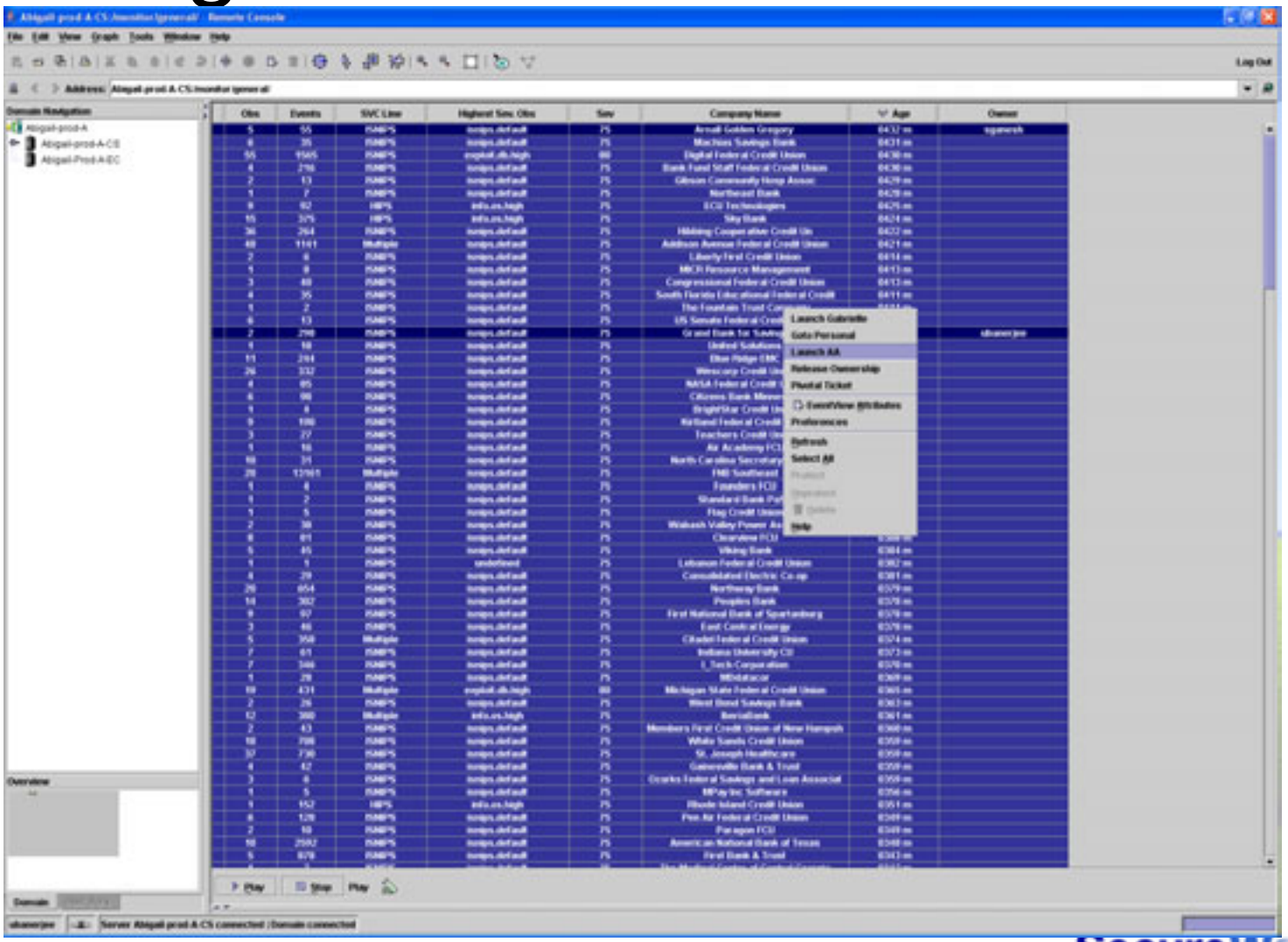
# Design Considerations

- 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

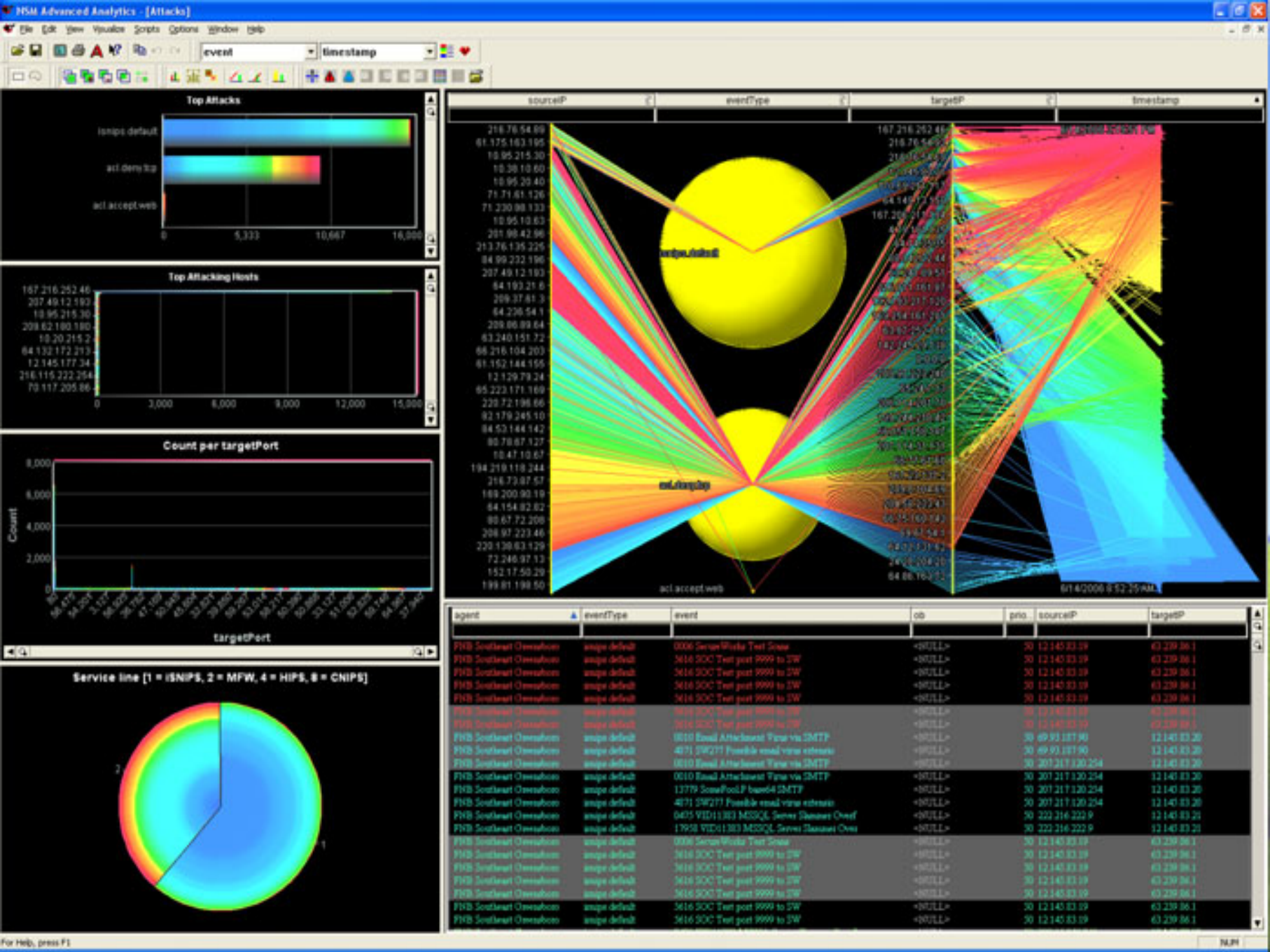
# Data Flow through the system

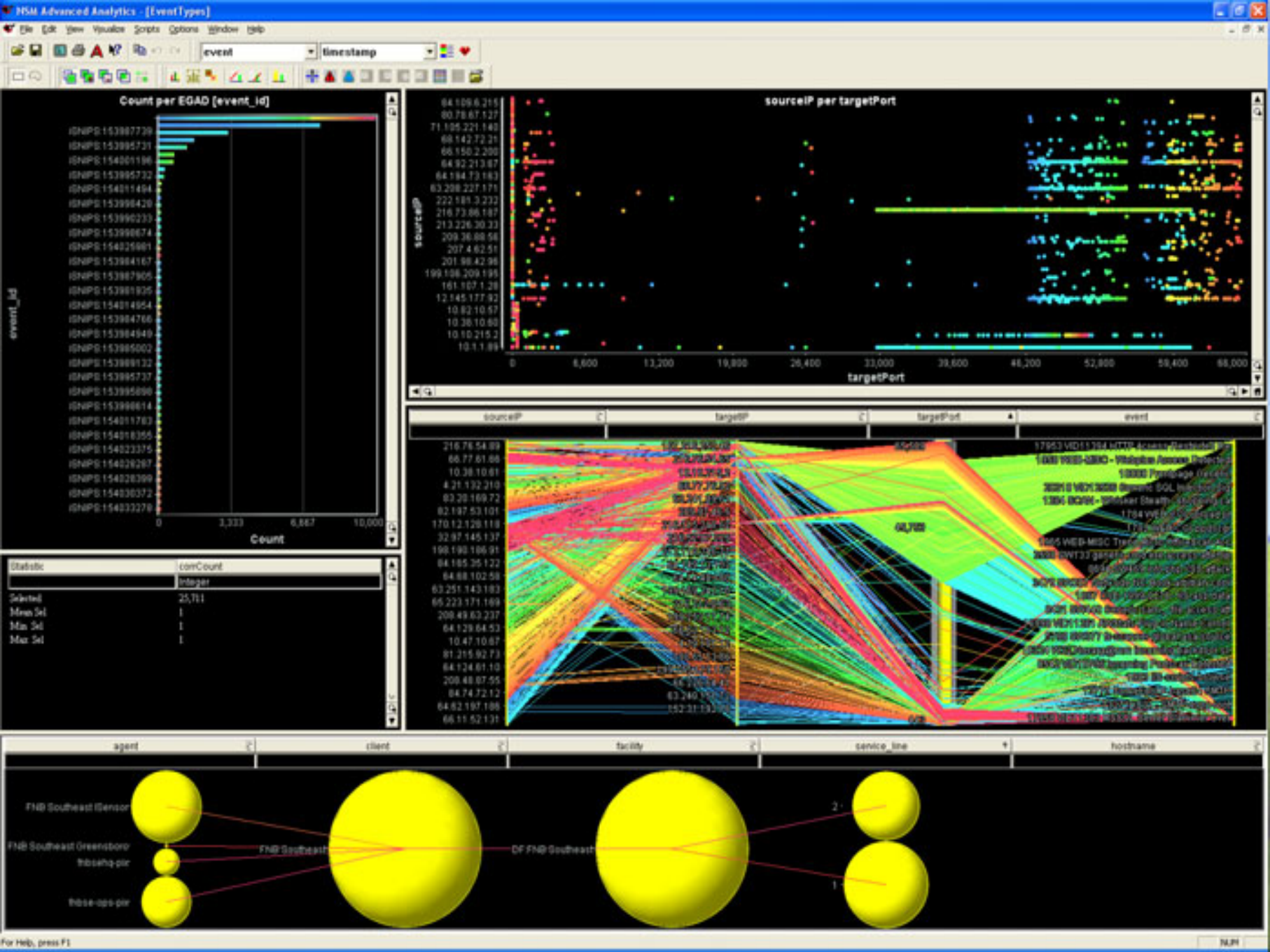


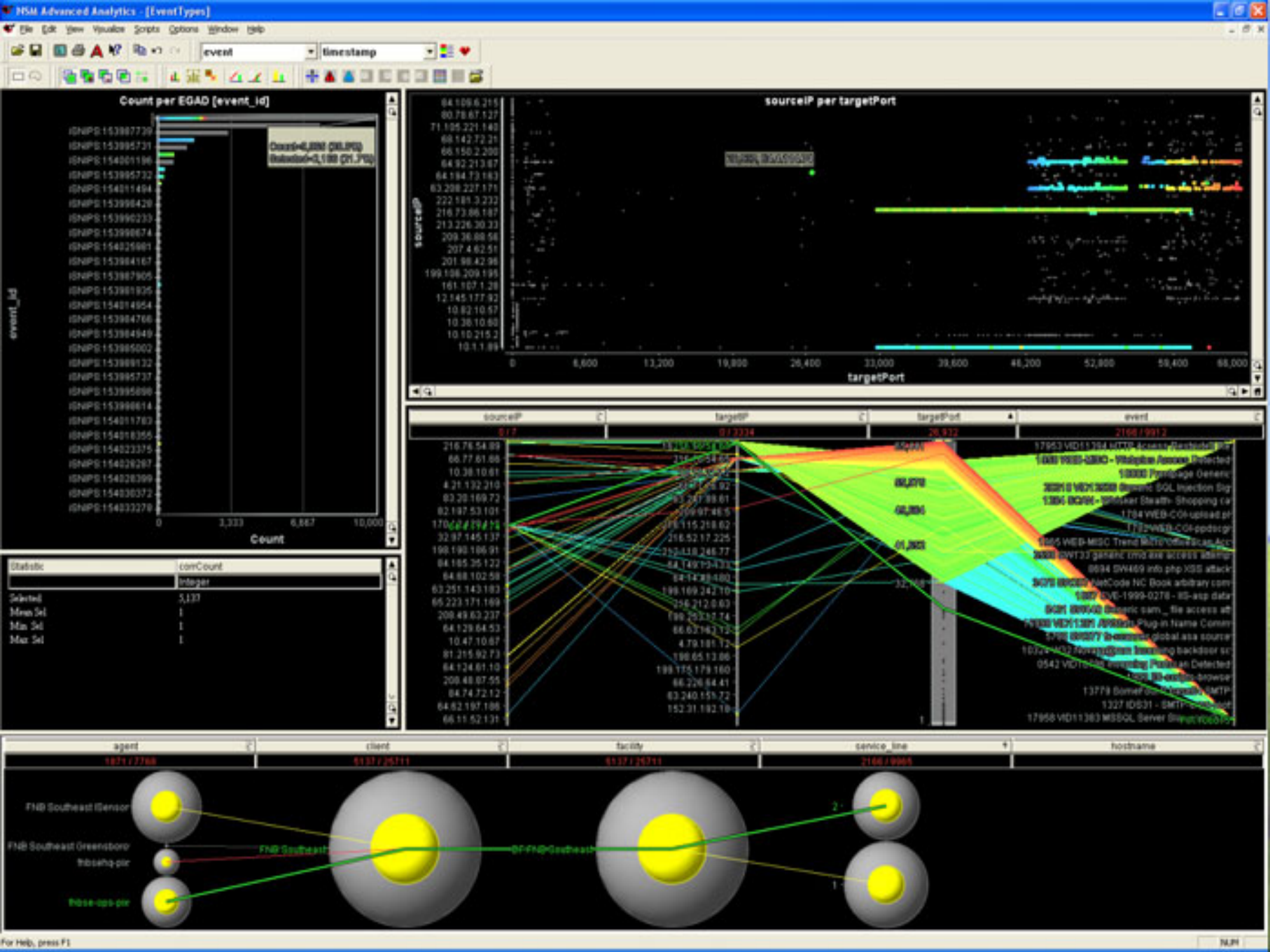
# Integration with our SIM Tool

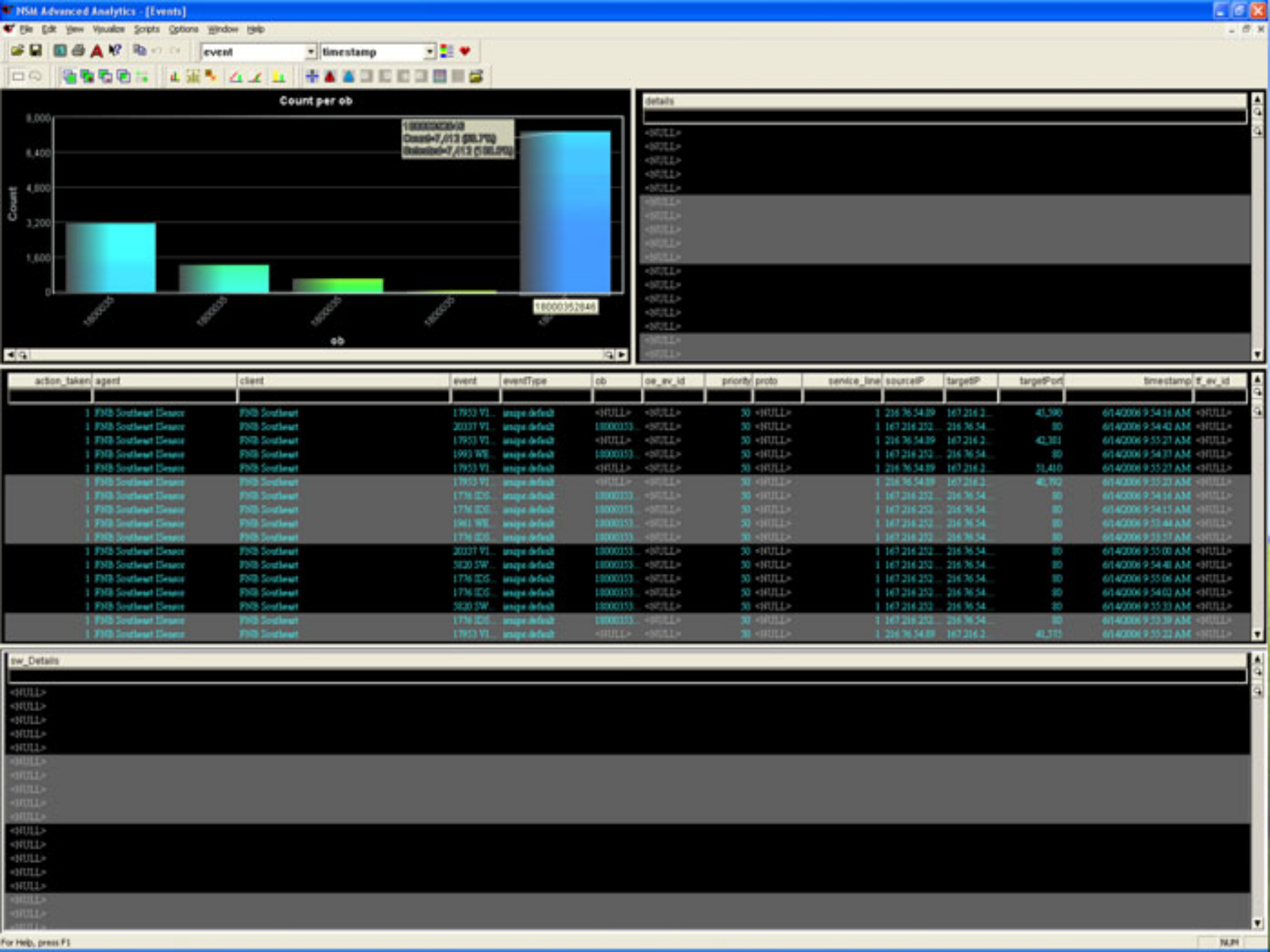


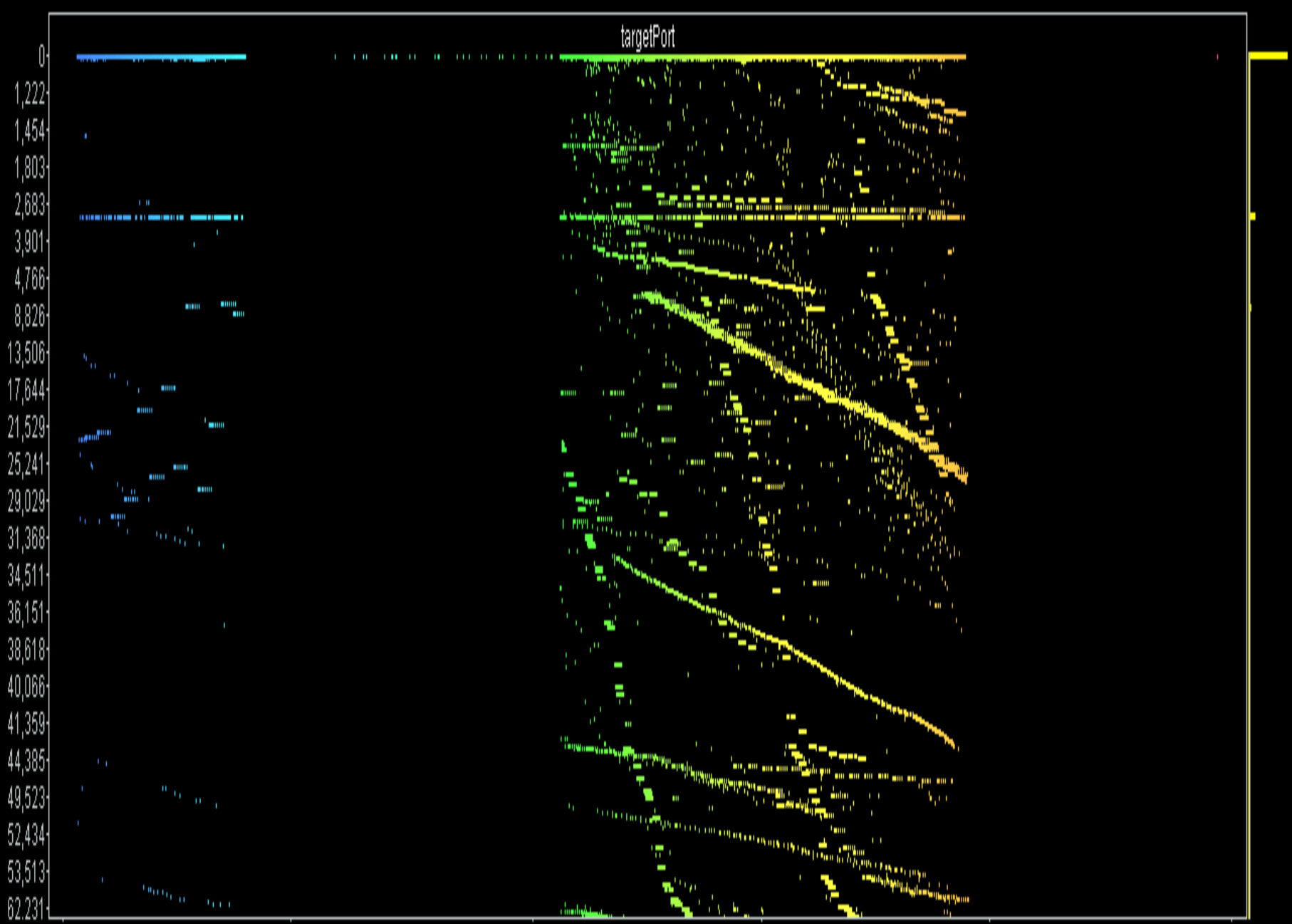
SecureWorks
The Information Security Experts

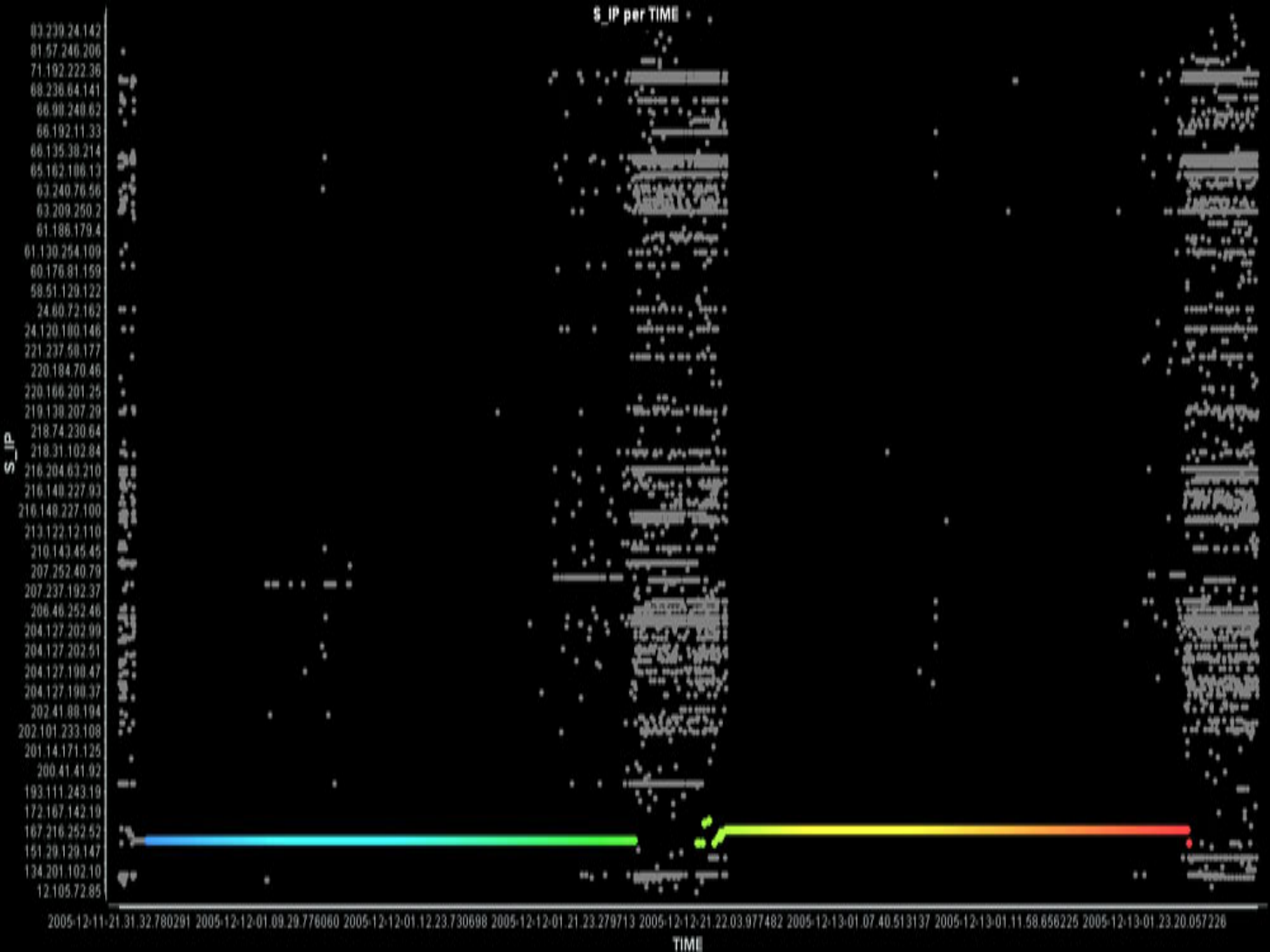

MSM Advanced Analytics - [Attacks]
File Edit View Visualize Scripts Options Window Help
event
timestamp
Top Attacks
isnips default
acl.deny.tcp
acl.accept.web
0
5,333
10,667
16,000
Top Attacking Hosts
167.216.252.46
207.49.12.193
10.95.215.30
209.62.180.180
10.20.215.2
64.132.172.213
12.145.177.34
216.115.222.254
70.117.205.86
0
3,000
6,000
9,000
12,000
15,000
Count per targetPort
8,000
6,000
4,000
2,000
0
Count
targetPort
Service line [1 = iSNIPS, 2 = MFW, 4 = HIPS, 8 = CNIPS]
sourceIP
eventType
targetIP
timestamp
acl.accept.web
agent
eventType
event
ob
prio
sourceIP
targetIP
For Help, press F1
NUM


NSM Advanced Analytics - [EventTypes]
File Edit View Visualize Scripts Options Window Help
event
timestamp
Count per EGAD [event_id]
event_id
Count
0
3,333
6,667
10,000
sourceIP per targetPort
sourceIP
targetPort
0
6,600
13,200
19,800
26,400
33,000
39,600
46,200
52,800
59,400
66,000
Statistic
corrCount
Integer
Selected
25,761
Mean Sel
1
Min Sel
1
Max Sel
1
sourceIP
targetIP
targetPort
event
agent
client
facility
service_line
hostname
FNB Southeast iSensor
FNB Southeast Greensboro
fnbsahq-pir
fnbse-ops-pir
FNB Southeast
DF FNB Southeast
For Help, press F1


NSM Advanced Analytics - [EventTypes]
File Edit View Visualize Scripts Options Window Help
event
timestamp
Count per EGAD [event_id]
event_id
Count
0
3,333
6,667
10,000
sourceIP per targetPort
sourceIP
targetPort
0
6,600
13,200
19,800
26,400
33,000
39,600
46,200
52,800
59,400
66,000
Statistic
corrCount
Integer
Selected
Mean Sel
Min Sel
Max Sel
sourceIP
targetIP
targetPort
event
agent
client
facility
service_line
hostname
FNB Southeast iSensor
FNB Southeast Greensboro
fnbsahq-pix
fnbse-ops-pix
FNB Southeast
For Help, press F1


HSM Advanced Analytics - [Events]
File Edit View Visualize Scripts Options Window Help
event
timestamp
Count per ob
Count
ob
details
action_taken agent client event eventType ob ce_av_id priority proto service_line sourceIP targetIP targetPort timestamp tf_av_id
sw_Details
For Help, press F1


targetPort
0
1,222
1,454
1,803
2,683
3,901
4,766
8,826
13,506
17,644
21,529
25,241
29,029
31,368
34,511
36,151
38,618
40,066
41,359
44,385
49,523
52,434
53,513
62,231
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
S_IP
03.230.24.142
01.57.246.206
71.192.222.36
68.236.64.141
66.90.240.62
66.192.11.33
66.135.38.214
65.162.106.13
63.240.76.56
63.209.250.2
61.186.179.4
61.130.254.109
60.176.81.159
58.51.120.122
24.60.72.162
24.120.180.146
221.237.58.177
220.184.70.46
220.166.201.25
219.138.207.29
218.74.230.64
218.31.102.84
216.204.63.210
216.140.227.93
216.140.227.100
213.122.12.110
210.143.45.45
207.252.40.79
207.237.192.37
206.46.252.46
204.127.202.99
204.127.202.51
204.127.198.47
204.127.198.37
202.41.88.194
202.101.233.108
201.14.171.125
200.41.41.92
193.111.243.19
172.167.142.19
167.216.252.52
151.29.120.147
134.201.102.10
12.105.72.85
2005-12-11-21.31.32.780291
2005-12-12-01.09.29.776060
2005-12-12-01.12.23.730698
2005-12-12-01.21.23.279713
2005-12-12-21.22.03.977482
2005-12-13-01.07.40.513137
2005-12-13-01.11.58.656225
2005-12-13-01.23.20.057226
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

SecureWorks
The Information Security Experts