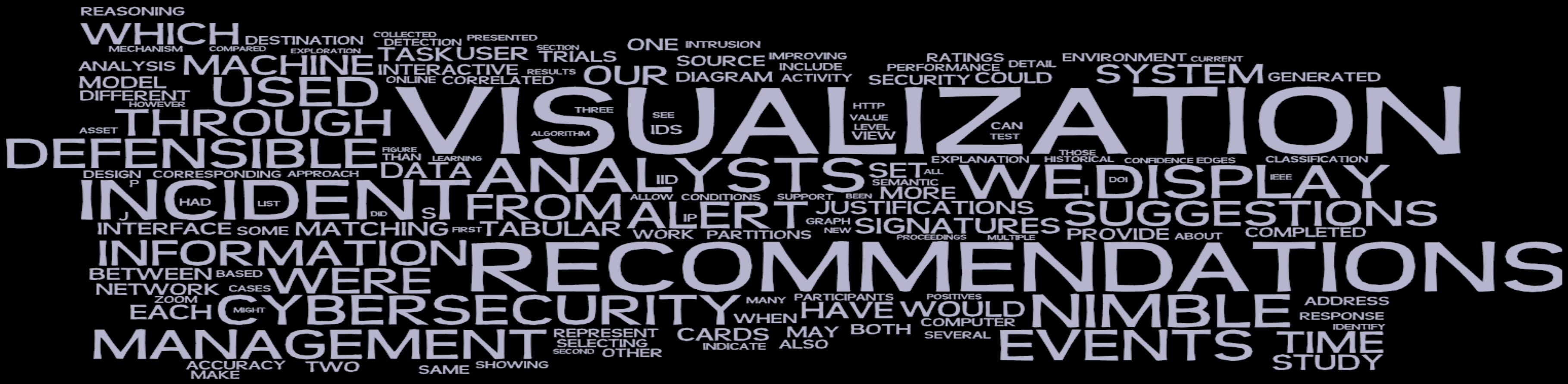
Jamie Rasmussen, IBM Research

14 September 2010

Nimble Cybersecurity Incident Management through Visualization and Defensible Recommendations



VizSec 2010

Jamie Rasmussen, IBM Research

14 September 2010

Nimble Cybersecurity Incident Management through Visualization and Defensible Recommendations

VizSec 2010

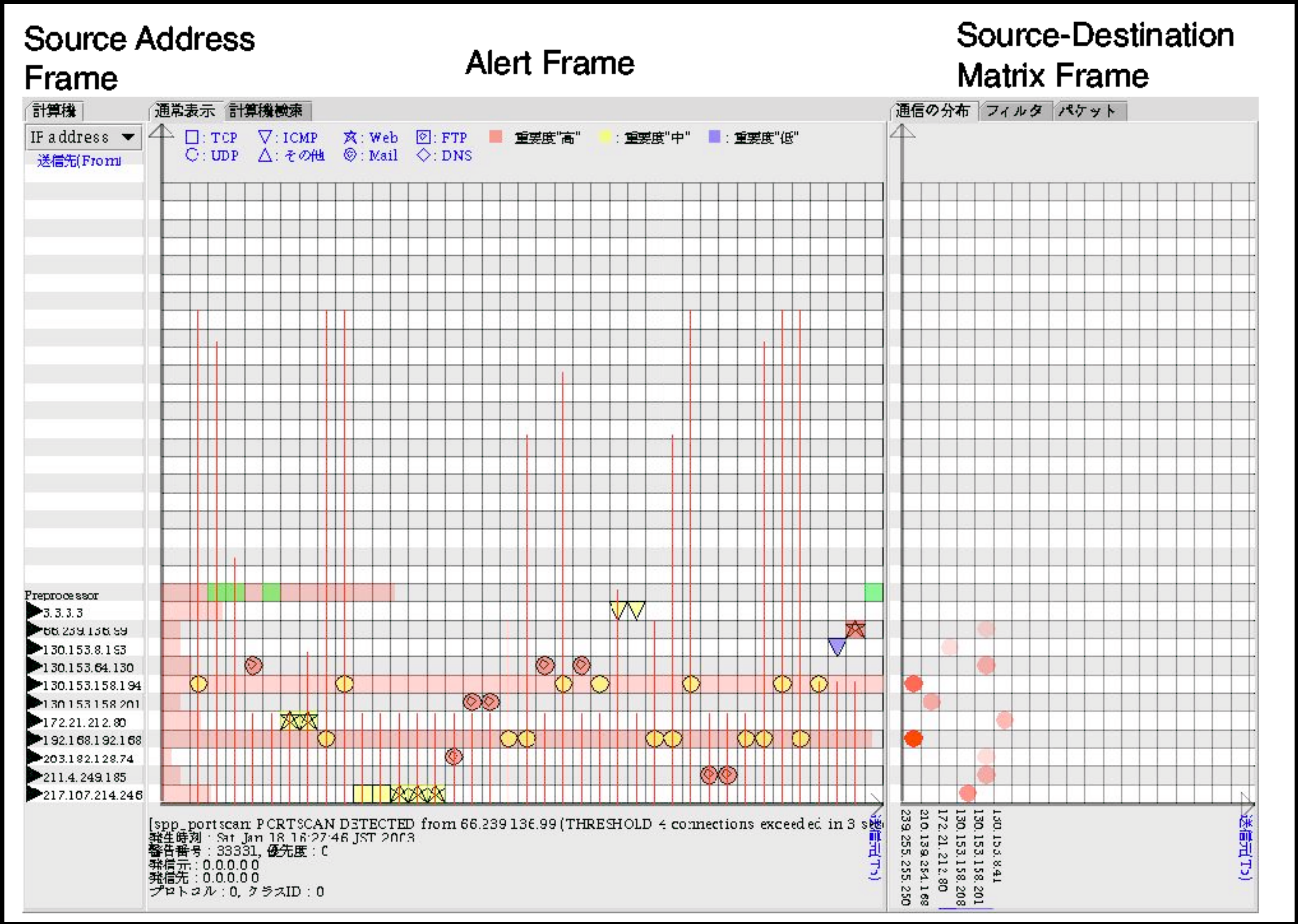
Our Goal

Help online analysts in Security Operations Centers complete their tasks more quickly and accurately

Our Approach

- An interactive graph-based visualization of correlated IDS output
- Defensible recommendations based on machine learning from historical analyst behavior
- Prototype tested with professional analysts in a controlled study

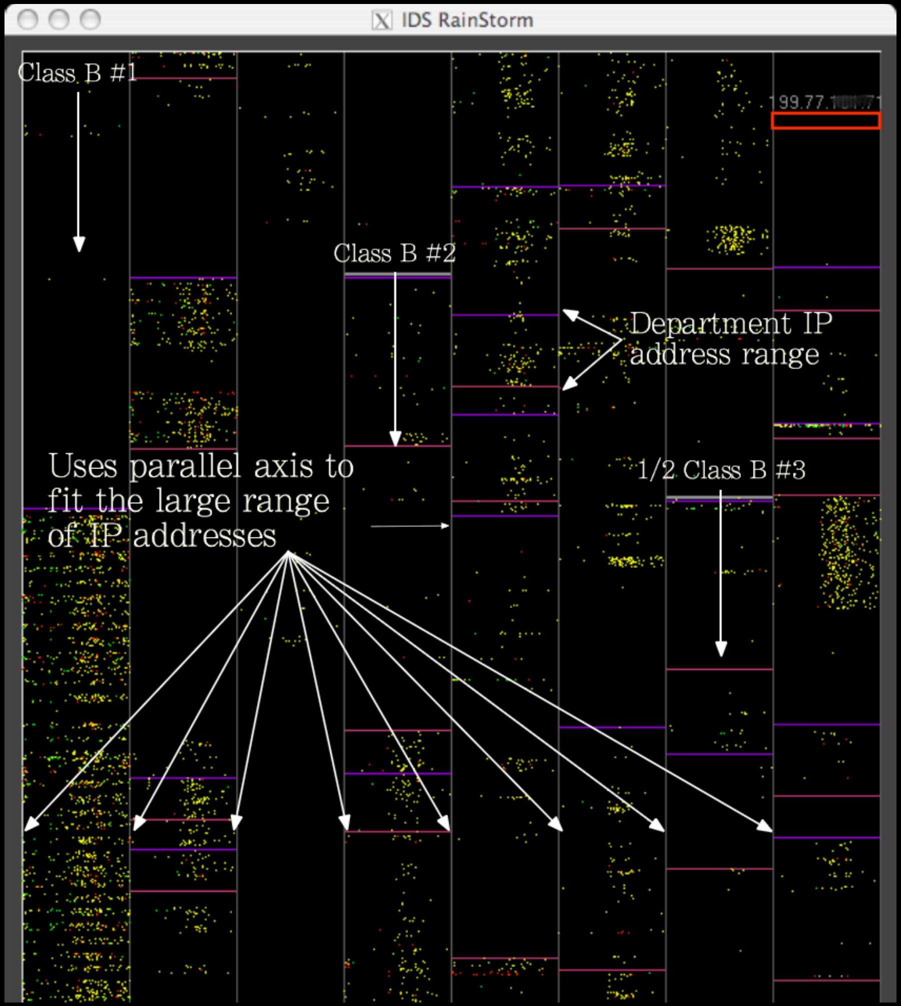
SnortView



```
[spp_portscan PORTSCAN DETECTED from 66.239.136.99 (THRESHOLD 4 connections exceeded in 3 se
発生時刻 : Sat Jan 18 16:27:46 JST 2003
警告番号 : 33331, 優先度 : 0
発信元 : 0.0.0.0 0
発信先 : 0.0.0.0 0
プロトコル : 0, クラスID : 0
```

Hideki Koike and Kazuhiro Ohno, VizSec 2004

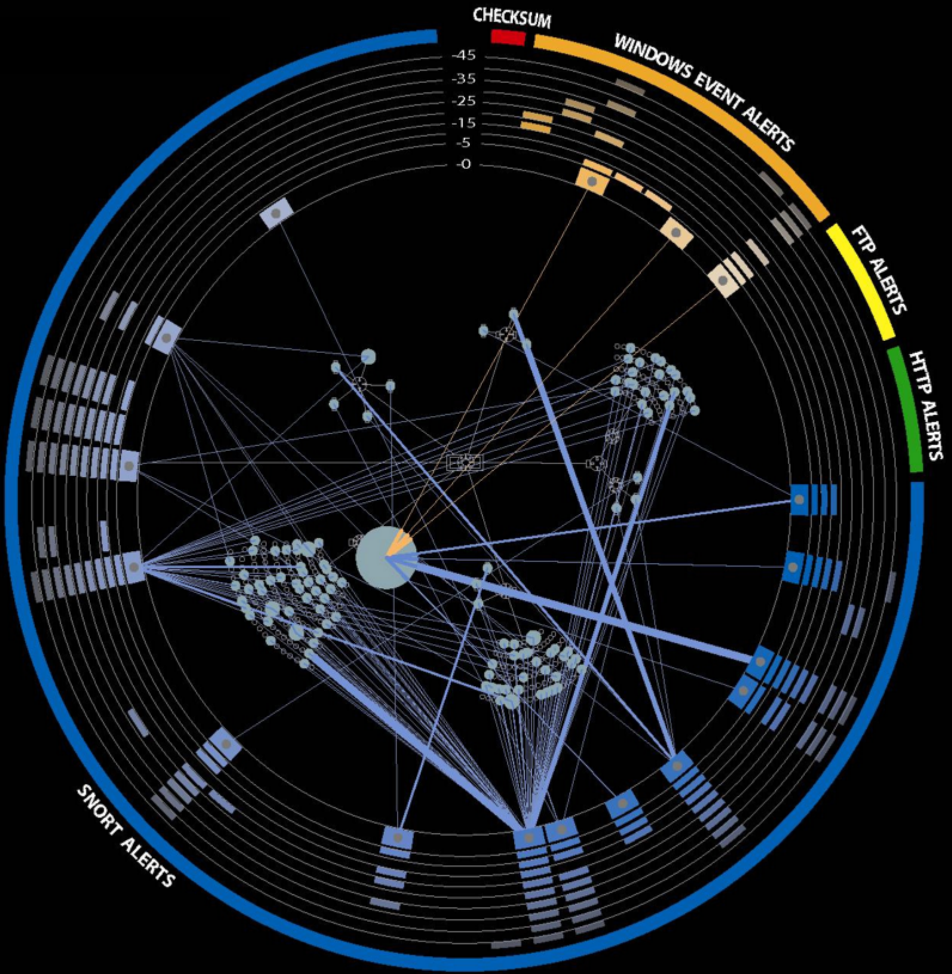
IDS RainStorm



Uses parallel axis to fit the large range of IP addresses

Kulsoom Abdullah et al., VizSec 2005

VisAlert

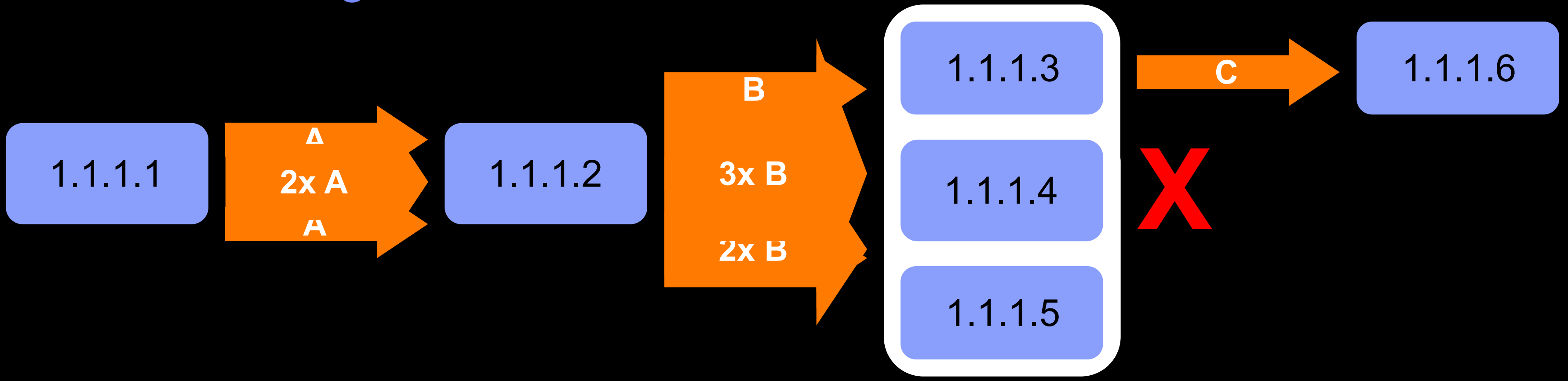


Yarden Livnat et al., 2005

Data Collection and Preparation

- **3** Monitored Organizations
- **8** Days
- **7** Sensors
- **2,869,108** IDS Events
- **164** Alerts
- **29** Analysts
- **106** Machines with Asset Information
- **No Identifying Information**
  - No plain text fields collected
  - IP addresses anonymized using Crypto-PAn
  - All unique identifiers replaced

Event Clustering

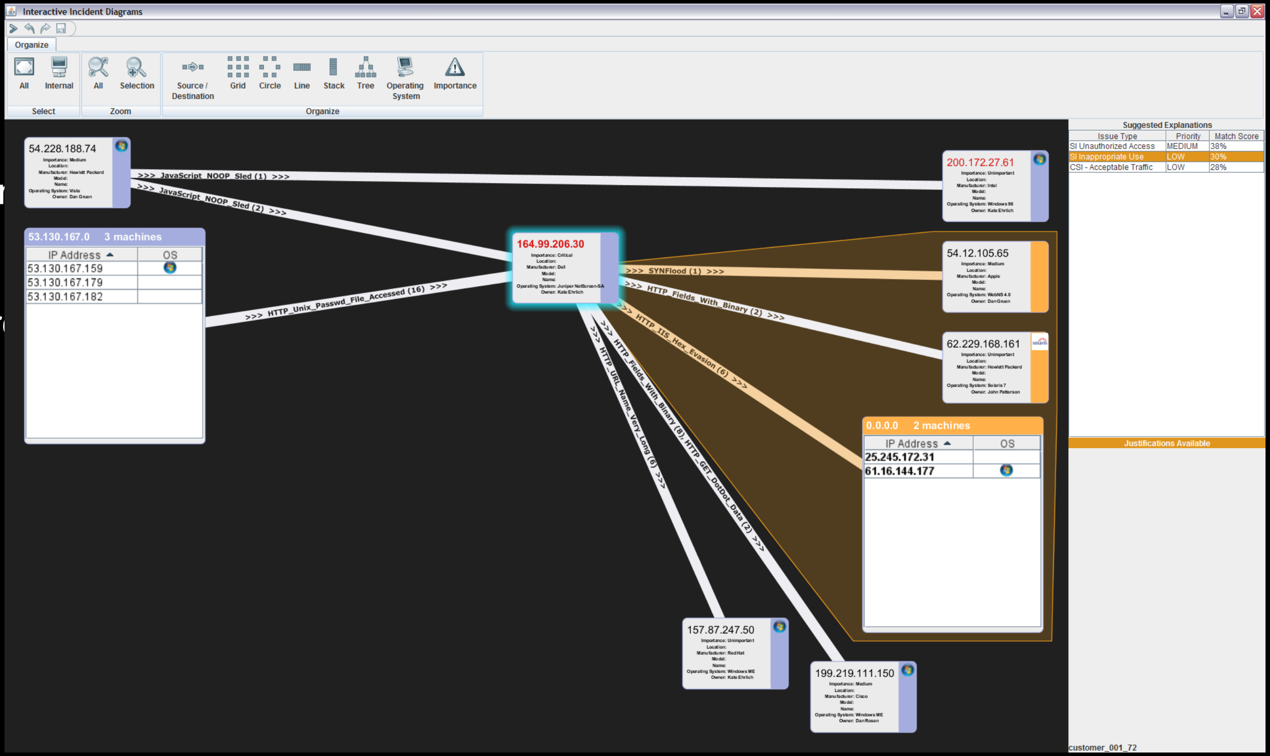


	Source	Signature	Destination
Partition 1	1.1.1.1	A	1.1.1.2
	1.1.1.1	A	1.1.1.2
Partition 2	1.1.1.2	B	1.1.1.3
Partition 3	1.1.1.2	B	1.1.1.4
	1.1.1.2	B	1.1.1.5
Partition 4	1.1.1.3	C	1.1.1.6

In each partition, each source must be connected
with each destination by each signature at least once

Interactive Incident Diagram (IID)

- Each partitio
- Sources and
- Multiple sour
- Visualization


Interactive Incident Diagrams
Organize
All
Internal
Select
All
Selection
Zoom
Source / Destination
Grid
Circle
Line
Stack
Tree
Operating System
Importance
Organize
>>> JavaScript_NOOP_Sled (1) >>>
>>> JavaScript_NOOP_Sled (2) >>>
>>> HTTP_Unix_Passwd_File_Accessed (16) >>>
>>> SYNFlood (1) >>>
>>> HTTP_Fields_With_Binary (2) >>>
>>> HTTP_IIS_Hex_Evasion (6) >>>
>>> HTTP_URL_Name_Very_Long (6) >>>
>>> HTTP_Fields_With_Binary (8), HTTP_GET_DotDot_Data (2) >>>
Justifications Available
customer_001_72

54.228.188.74
Importance: Medium
Location:
Manufacturer: Hewlett Packard
Model:
Name:
Operating System: Vista
Owner: Dan Gruen

53.130.167.0 3 machines

IP Address ▲	OS
53.130.167.159	⊞
53.130.167.179	
53.130.167.182	

164.99.206.30
Importance: Critical
Location:
Manufacturer: Dell
Model:
Name:
Operating System: Juniper NetScreen-SA
Owner: Kate Ehrlich

200.172.27.61
Importance: Unimportant
Location:
Manufacturer: Intel
Model:
Name:
Operating System: Windows 98
Owner: Kate Ehrlich

54.12.105.65
Importance: Medium
Location:
Manufacturer: Apple
Model:
Name:
Operating System: WebNS 4.0
Owner: Dan Gruen

62.229.168.161
Importance: Unimportant
Location:
Manufacturer: Hewlett Packard
Model:
Name:
Operating System: Solaris 7
Owner: John Patterson

0.0.0.0 2 machines

IP Address ▲	OS
25.245.172.31	
61.16.144.177	⊞

157.87.247.50
Importance: Unimportant
Location:
Manufacturer: Red Hat
Model:
Name:
Operating System: Windows ME
Owner: Kate Ehrlich

199.219.111.150
Importance: Medium
Location:
Manufacturer: Cisco
Model:
Name:
Operating System: Windows ME
Owner: Dan Rosen

Suggested Explanations

Issue Type	Priority	Match Score
SI Unauthorized Access	MEDIUM	38%
SI Inappropriate Use	LOW	30%
CSI - Acceptable Traffic	LOW	28%

Research Questions

- Is diagnosis better with this interactive visualization than a tabular display?
- Will analysts benefit from the display of classification recommendations?
- Will the benefits depend on whether the recommendations are accompanied by justifications?

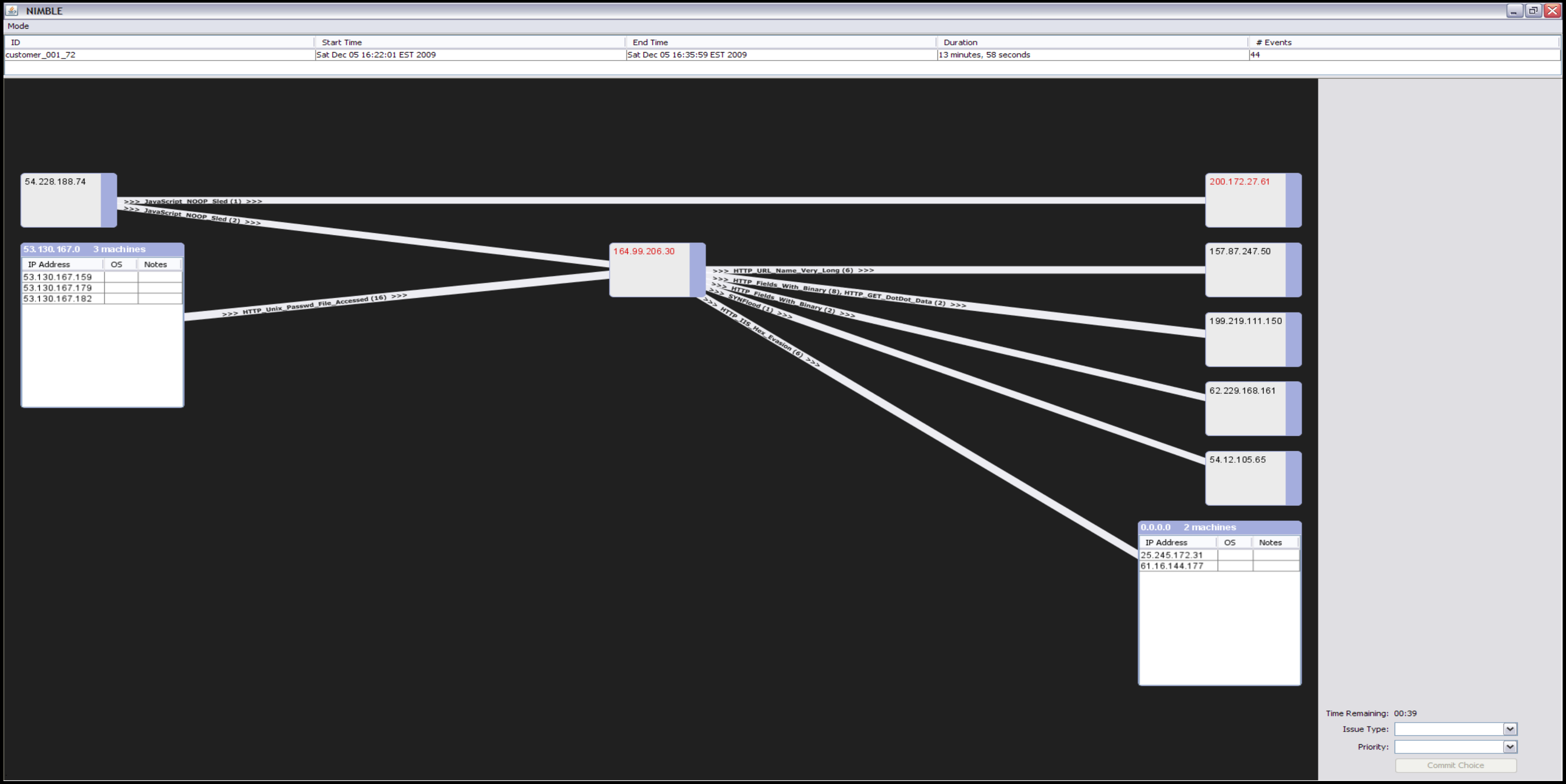
The Study

- Participants
  - 18 professional security analysts
  - Minimum of three years experience, most had over five
- Each participant completes 24 trials. For each trial:
  - Analyst presented information about an alert
  - Asked to classify it with regards to issue type and priority
  - Two minute time limit with audible warnings
  - Once they have classified it indicate their confidence in their judgment
  - “Talk-Aloud” protocol
- After trials, participants completed a survey
- Discussion with all participants in a group debrief session

The Study

- Four experimental conditions
  - Presentation of Events: Visual or Tabular
  - Recommendation: No Suggestions, 3 Suggestions, or 3 Suggestions with Justifications
  - Correct Suggestion Available: Yes or No
  - Block of Trials: First or Second
- Measurements
  - **Accuracy** of response
  - **Time** to complete problem
  - **Confidence** in response
  - **Ratings** from survey

Visual Display


NIMBLE
Mode
54.228.188.74
200.172.27.61
164.99.206.30
157.87.247.50
199.219.111.150
62.229.168.161
54.12.105.65
>>> JavaScript_NOOP_Sled (1) >>>
>>> JavaScript_NOOP_Sled (2) >>>
>>> HTTP_Unix_Passwd_File_Accessed (16) >>>
>>> HTTP_URL_Name_Very_Long (6) >>>
>>> HTTP_Fields_With_Binary (8), HTTP_GET_DotDot_Data (2) >>>
>>> HTTP_Fields_With_Binary (2) >>>
>>> SYNFlood (1) >>>
>>> HTTP_IIS_Hex_Evasion (6) >>>
Commit Choice

ID	Start Time	End Time	Duration	# Events
customer_001_72	Sat Dec 05 16:22:01 EST 2009	Sat Dec 05 16:35:59 EST 2009	13 minutes, 58 seconds	44

53.130.167.0 3 machines

IP Address	OS	Notes
53.130.167.159		
53.130.167.179		
53.130.167.182		

0.0.0.0 2 machines

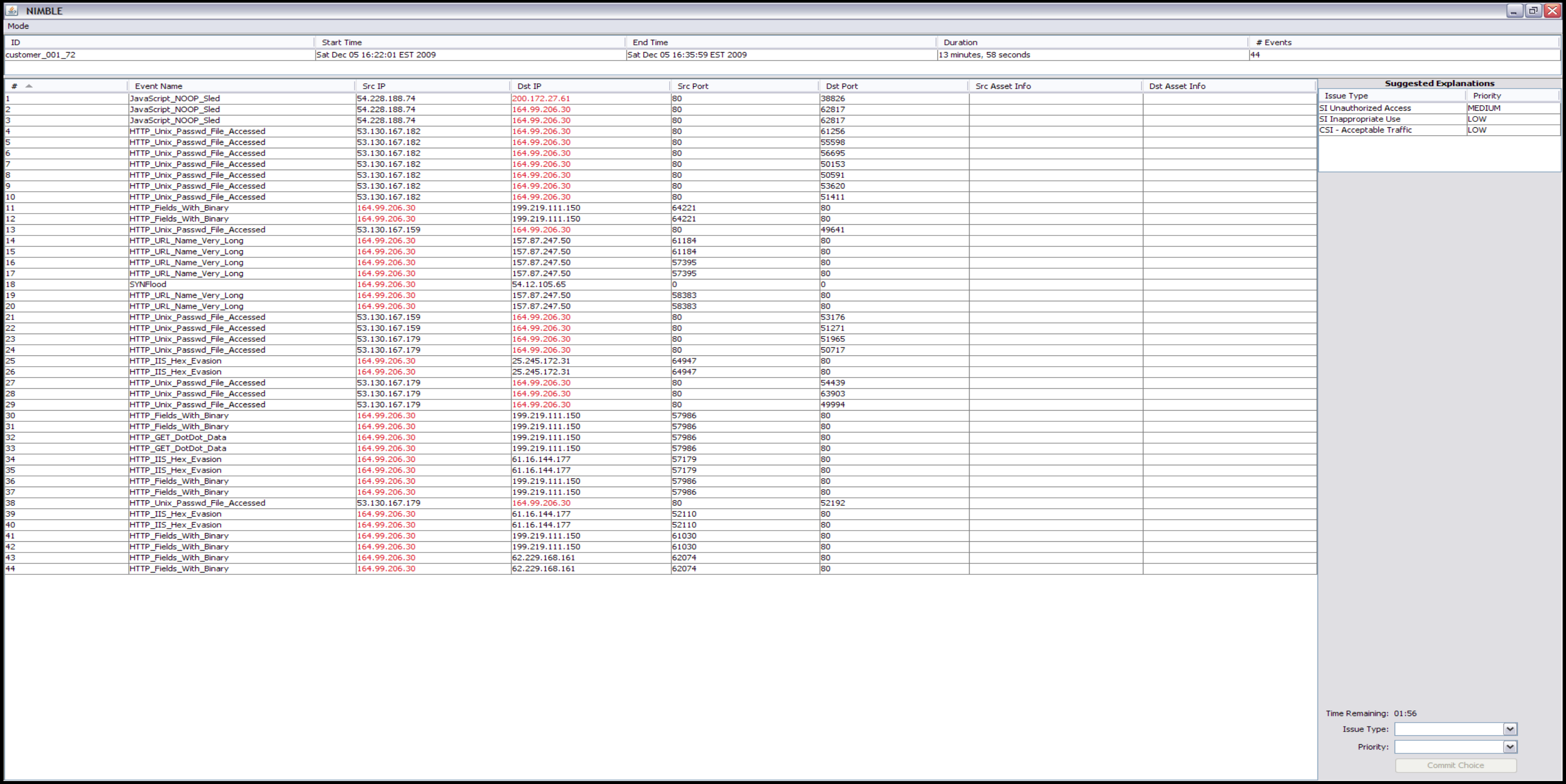
IP Address	OS	Notes
25.245.172.31		
61.16.144.177		

Time Remaining: 00:39

Issue Type:

Priority:

Tabular Display with Suggestion



ID	Start Time	End Time	Duration	# Events
customer_001_72	Sat Dec 05 16:22:01 EST 2009	Sat Dec 05 16:35:59 EST 2009	13 minutes, 58 seconds	44

#	Event Name	Src IP	Dst IP	Src Port	Dst Port	Src Asset Info	Dst Asset Info
1	JavaScript_NOOP_Sled	54.228.188.74	200.172.27.61	80	38826		
2	JavaScript_NOOP_Sled	54.228.188.74	164.99.206.30	80	62817		
3	JavaScript_NOOP_Sled	54.228.188.74	164.99.206.30	80	62817		
4	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	61256		
5	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	55598		
6	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	56695		
7	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	50153		
8	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	50591		
9	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	53620		
10	HTTP_Unix_Passwd_File_Accessed	53.130.167.182	164.99.206.30	80	51411		
11	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	64221	80		
12	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	64221	80		
13	HTTP_Unix_Passwd_File_Accessed	53.130.167.159	164.99.206.30	80	49641		
14	HTTP_URL_Name_Very_Long	164.99.206.30	157.87.247.50	61184	80		
15	HTTP_URL_Name_Very_Long	164.99.206.30	157.87.247.50	61184	80		
16	HTTP_URL_Name_Very_Long	164.99.206.30	157.87.247.50	57395	80		
17	HTTP_URL_Name_Very_Long	164.99.206.30	157.87.247.50	57395	80		
18	SYNFlood	164.99.206.30	54.12.105.65	0	0		
19	HTTP_URL_Name_Very_Long	164.99.206.30	157.87.247.50	58383	80		
20	HTTP_URL_Name_Very_Long	164.99.206.30	157.87.247.50	58383	80		
21	HTTP_Unix_Passwd_File_Accessed	53.130.167.159	164.99.206.30	80	53176		
22	HTTP_Unix_Passwd_File_Accessed	53.130.167.159	164.99.206.30	80	51271		
23	HTTP_Unix_Passwd_File_Accessed	53.130.167.179	164.99.206.30	80	51965		
24	HTTP_Unix_Passwd_File_Accessed	53.130.167.179	164.99.206.30	80	50717		
25	HTTP_IIS_Hex_Evasion	164.99.206.30	25.245.172.31	64947	80		
26	HTTP_IIS_Hex_Evasion	164.99.206.30	25.245.172.31	64947	80		
27	HTTP_Unix_Passwd_File_Accessed	53.130.167.179	164.99.206.30	80	54439		
28	HTTP_Unix_Passwd_File_Accessed	53.130.167.179	164.99.206.30	80	63903		
29	HTTP_Unix_Passwd_File_Accessed	53.130.167.179	164.99.206.30	80	49994		
30	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	57986	80		
31	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	57986	80		
32	HTTP_GET_DotDot_Data	164.99.206.30	199.219.111.150	57986	80		
33	HTTP_GET_DotDot_Data	164.99.206.30	199.219.111.150	57986	80		
34	HTTP_IIS_Hex_Evasion	164.99.206.30	61.16.144.177	57179	80		
35	HTTP_IIS_Hex_Evasion	164.99.206.30	61.16.144.177	57179	80		
36	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	57986	80		
37	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	57986	80		
38	HTTP_Unix_Passwd_File_Accessed	53.130.167.179	164.99.206.30	80	52192		
39	HTTP_IIS_Hex_Evasion	164.99.206.30	61.16.144.177	52110	80		
40	HTTP_IIS_Hex_Evasion	164.99.206.30	61.16.144.177	52110	80		
41	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	61030	80		
42	HTTP_Fields_With_Binary	164.99.206.30	199.219.111.150	61030	80		
43	HTTP_Fields_With_Binary	164.99.206.30	62.229.168.161	62074	80		
44	HTTP_Fields_With_Binary	164.99.206.30	62.229.168.161	62074	80		

Suggested Explanations

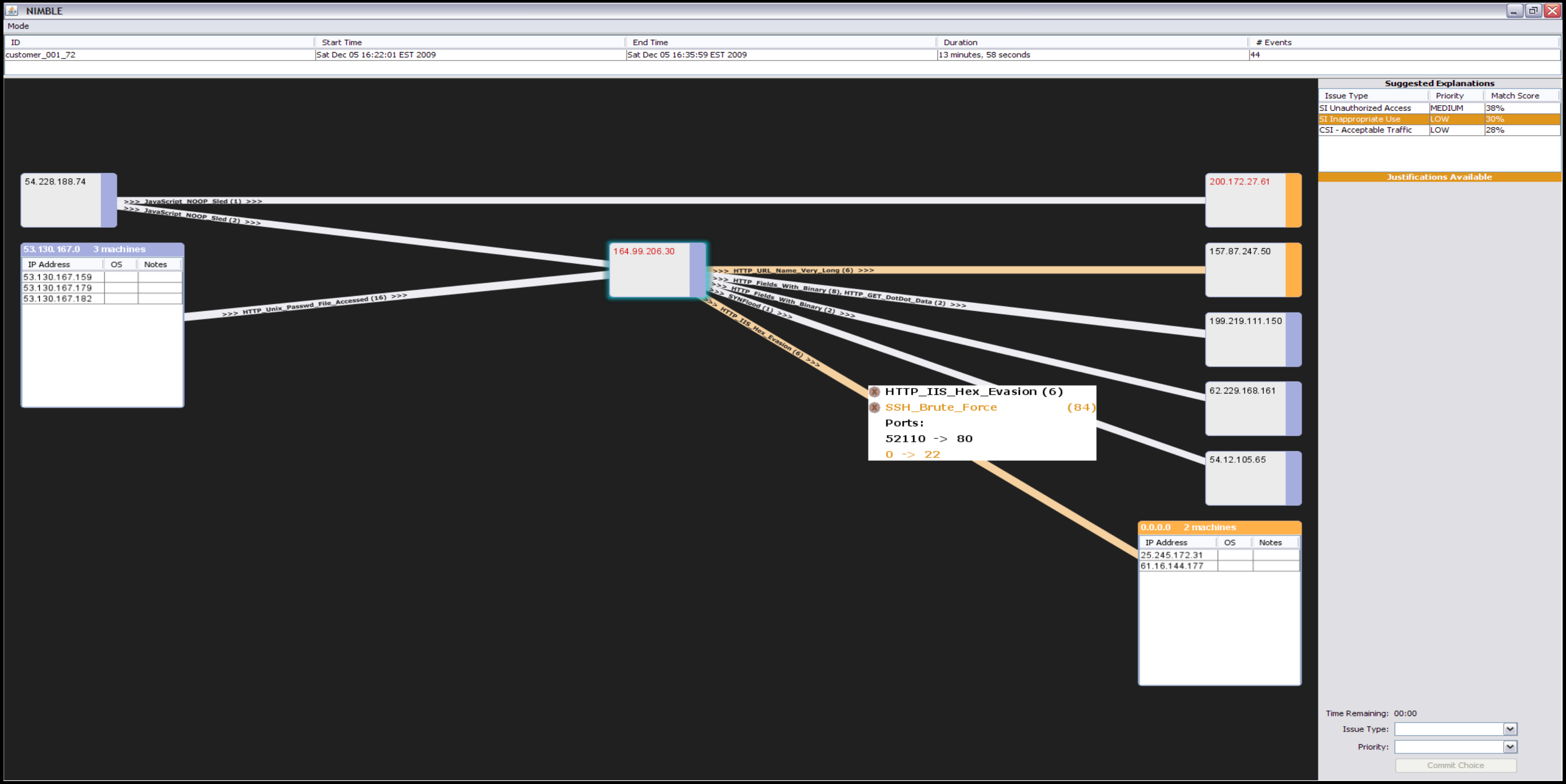
Issue Type	Priority
SI Unauthorized Access	MEDIUM
SI Inappropriate Use	LOW
CSI - Acceptable Traffic	LOW

Time Remaining: 01:56

Issue Type:

Priority:

Visual Display with Justification



NIMBLE

Mode

ID	Start Time	End Time	Duration	# Events
customer_001_72	Sat Dec 05 16:22:01 EST 2009	Sat Dec 05 16:35:59 EST 2009	13 minutes, 58 seconds	44

Suggested Explanations

Issue Type	Priority	Match Score
SI Unauthorized Access	MEDIUM	38%
SI Inappropriate Use	LOW	30%
CSI - Acceptable Traffic	LOW	28%

Justifications Available

53.130.167.0 3 machines

IP Address	OS	Notes
53.130.167.159		
53.130.167.179		
53.130.167.182		

0.0.0.0 2 machines

IP Address	OS	Notes
25.245.172.31		
61.16.144.177		

HTTP_IIS_Hex_Evasion (6)
SSH_Brute_Force (84)
Ports:
52110 -> 80
0 -> 22

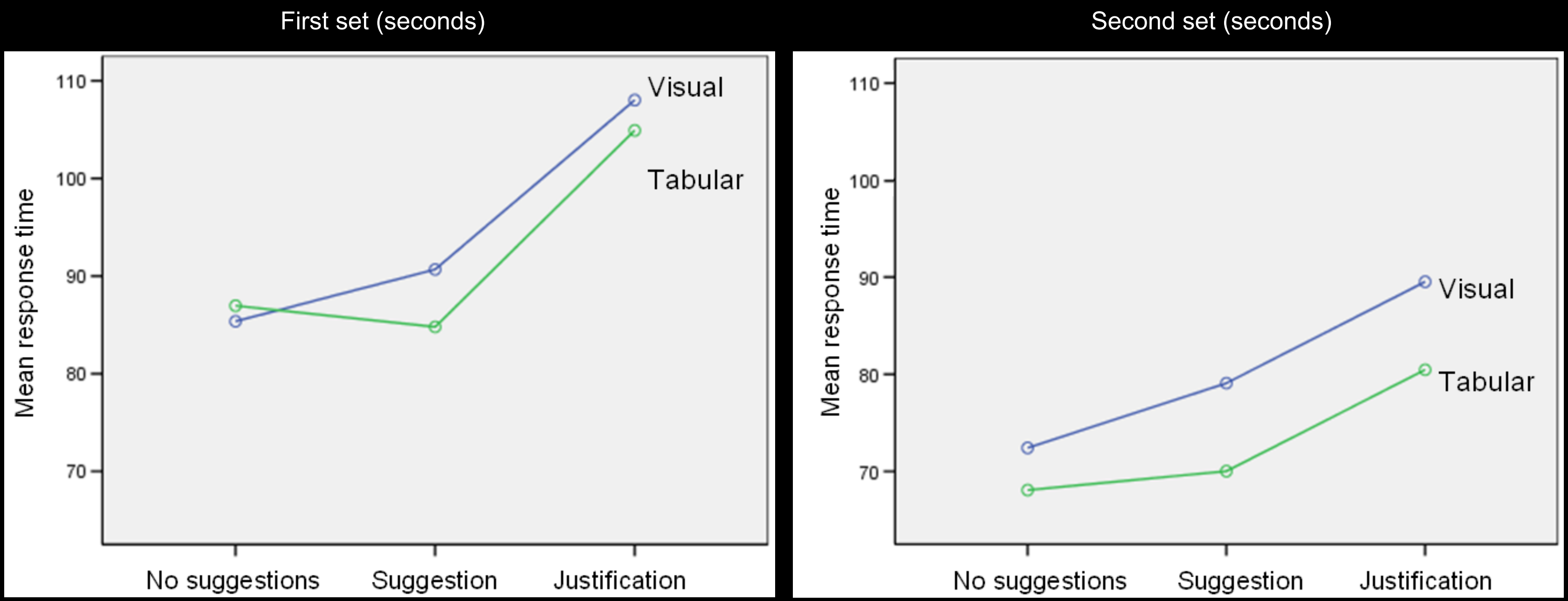
Time Remaining: 00:00

Issue Type:

Priority:

54.228.188.74
>>> JavaScript_NOOP_Sled (1) >>>
>>> JavaScript_NOOP_Sled (2) >>>
>>> HTTP_Unix_Passwd_File_Accessed (16) >>>
164.99.206.30
>>> HTTP_URL_Name_Very_Long (6) >>>
>>> HTTP_Fields_With_Binary (8), HTTP_GET_DotDot_Data (2) >>>
>>> HTTP_Fields_With_Binary (2) >>>
>>> SYNFlood (1) >>>
>>> HTTP_IIS_Hex_Evasion (6) >>>
200.172.27.61
157.87.247.50
199.219.111.150
62.229.168.161
54.12.105.65
Commit Choice

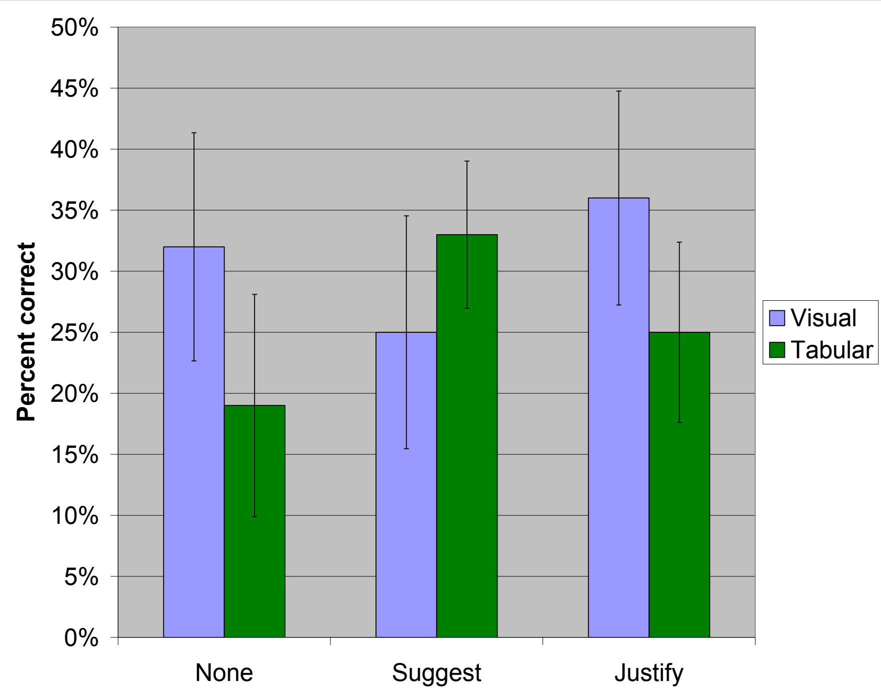
Response Time Across Display and Recommendation Conditions


First set (seconds)

Second set (seconds)

- First set took longer overall than second set ($p < 0.01$)
- Justifications and suggestions took longer than baseline ($p < 0.01$)
- Visual displays took slightly longer than the tabular displays ($p = 0.12$)

Accuracy Across Display and Recommendation Conditions



- Slightly higher accuracy associated with visual (31%) than tabular (26%) across all recommendation conditions ($p < 0.10$)
- Effect stronger in second half, accuracy with visual was 35%, tabular was 20% ($p < 0.05$)
- Across both display types, there was no overall difference between the three level of recommendation ($p > 0.10$)

Research Questions Revisited

- Is diagnosis better with this interactive visualization than a tabular display?
  - ➢ Analysts were more accurate with the visualization, slightly slower
  - ➢ Two “camps”, strong proponents for both kinds of display

- Will analysts benefit from the display of classification recommendations?
  - ➢ Analysts were slower when recommendations shown, no impact on accuracy
  - ➢ The prevalence of incorrect recommendations may have reduced utility

- Will the benefits depend on whether the recommendations are accompanied by justifications?
  - ➢ Individual ratings for justifications significantly higher than for suggestions
  - ➢ Preference for justifications increased with tenure

Thank You!

Jamie Rasmussen
Software Engineer
jrasmus@us.ibm.com

Kate Ehrlich
Research Scientist
katee@us.ibm.com

Steven Ross
Technical Lead
Steven_Ross@us.ibm.com

Susanna Kirk
Student Intern
sekirk@us.ibm.com

Dan Gruen
Research Scientist
Daniel_Gruen@us.ibm.com

John Patterson
Manager & Distinguished Engineer
John_Patterson@us.ibm.com