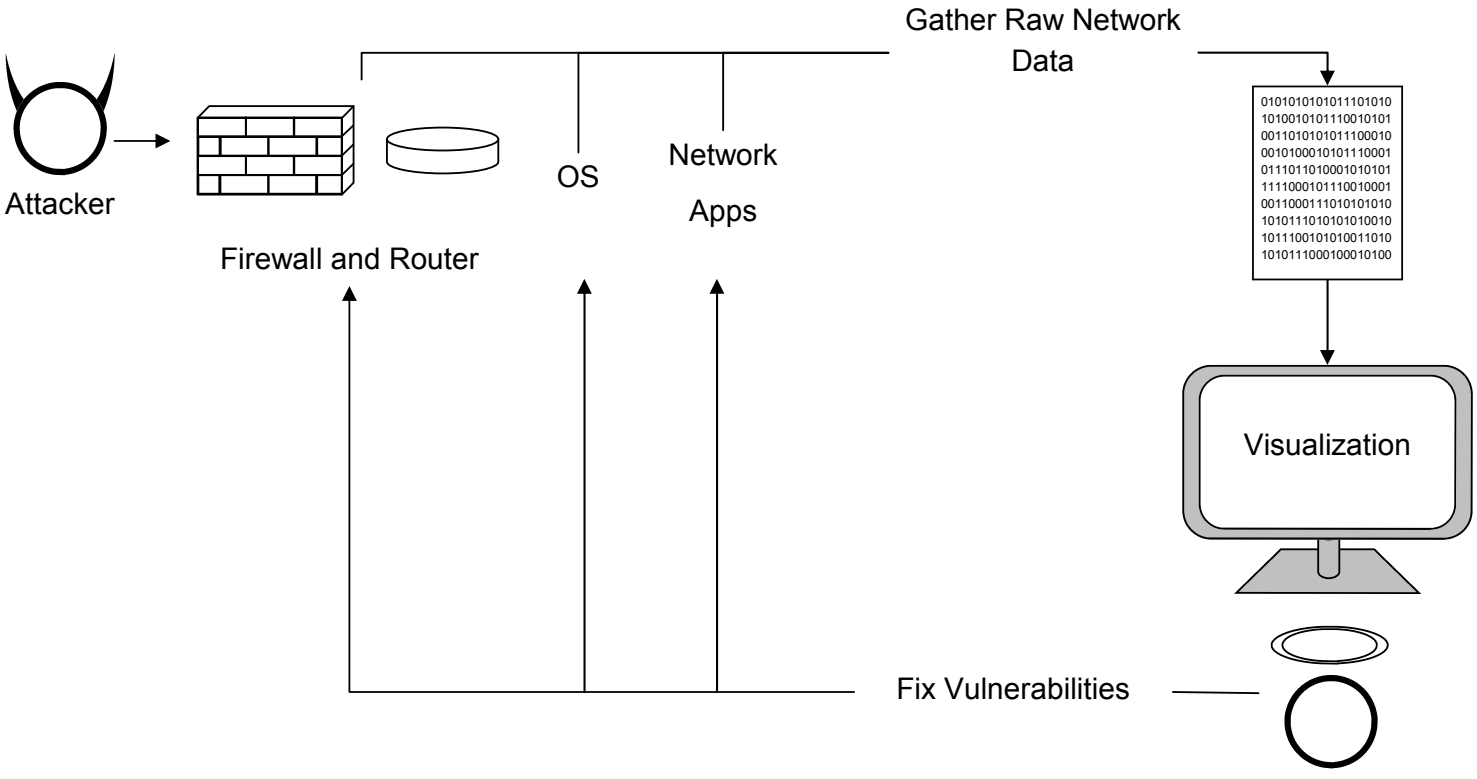
Network Security Visualization

Genevieve Max & Keith Fligg

April 22, 2012

Attack Scenario



Three Ws of Tool Design

1. *Where* in the network is the attack happening?

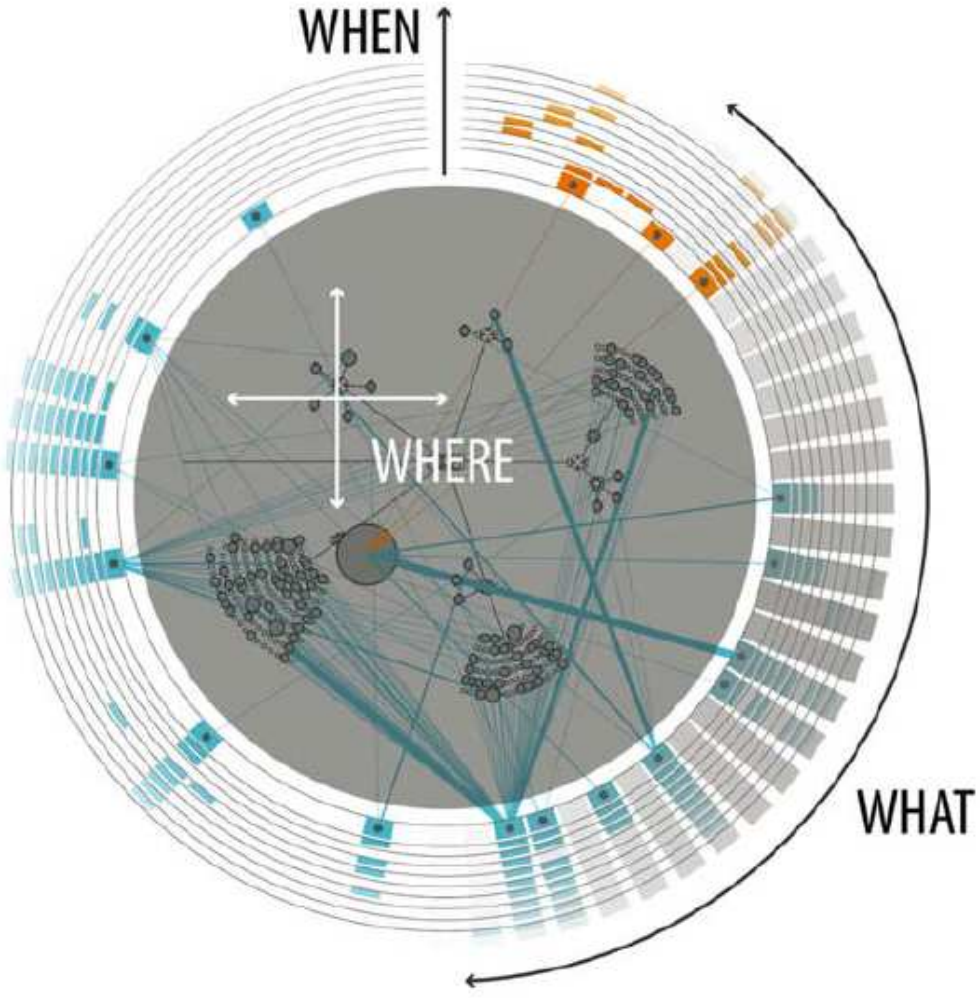
Three Ws of Tool Design

1. *Where* in the network is the attack happening?
2. *When* is the attack happening?

Three Ws of Tool Design

1. *Where* in the network is the attack happening?
2. *When* is the attack happening?
3. *What* type of attack is happening?

Visualization Answering Three Ws



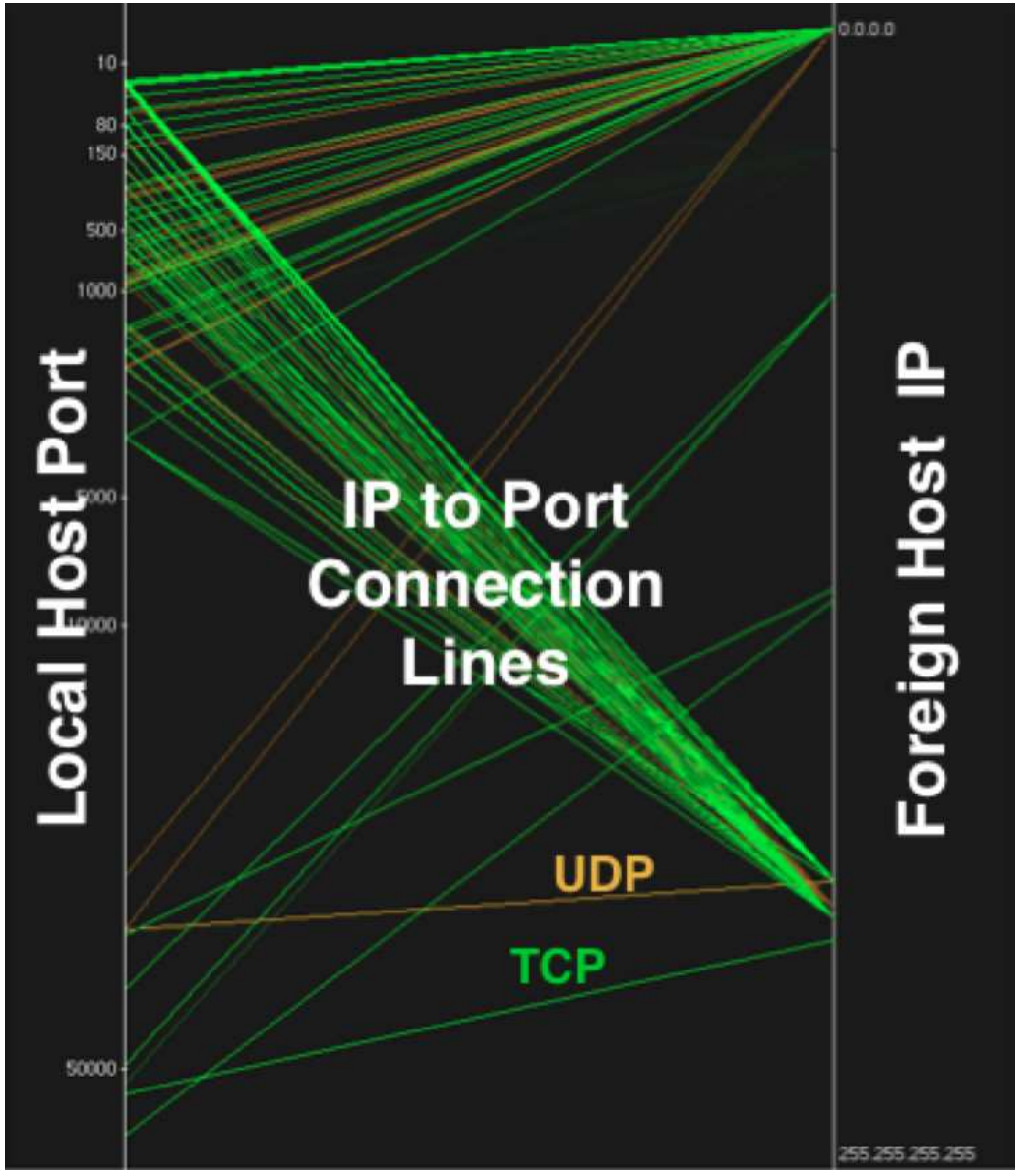
Firewall Log

```
6:12:04 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:64254 from 10.0.1.1:53
6:12:14 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:63828 from 10.0.1.1:53
6:12:24 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:62285 from 10.0.1.1:53
6:13:03 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:54340 from 10.0.1.1:53
6:13:43 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:61731 from 10.0.1.1:53
6:13:53 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:49345 from 10.0.1.1:53
6:14:23 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:53758 from 10.0.1.1:53
6:14:26 PM Firewall: Stealth Mode connection attempt to TCP 10.0.1.4:64906 from 58.254.109.182:1038
6:14:29 PM Firewall: Stealth Mode connection attempt to TCP 10.0.1.4:64906 from 58.254.109.182:1038
6:14:35 PM Firewall: Stealth Mode connection attempt to TCP 10.0.1.4:64906 from 58.254.109.182:1038
6:14:56 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:51553 from 10.0.1.1:53
6:15:03 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:52059 from 10.0.1.1:53
6:15:33 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:51553 from 10.0.1.1:53
6:15:53 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:54117 from 10.0.1.1:53
6:16:53 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:52363 from 10.0.1.1:53
6:17:44 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:65324 from 10.0.1.1:53
6:18:54 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:57882 from 10.0.1.1:53
6:19:14 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:61798 from 10.0.1.1:53
6:19:44 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:56687 from 10.0.1.1:53
6:19:45 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:55394 from 10.0.1.1:53
6:19:56 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:57937 from 10.0.1.1:53
6:20:46 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:63449 from 10.0.1.1:53
6:20:54 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:59261 from 10.0.1.1:53
6:21:13 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:64629 from 10.0.1.1:53
6:21:33 PM Firewall: Stealth Mode connection attempt to UDP 10.0.1.4:64917 from 10.0.1.1:53
```

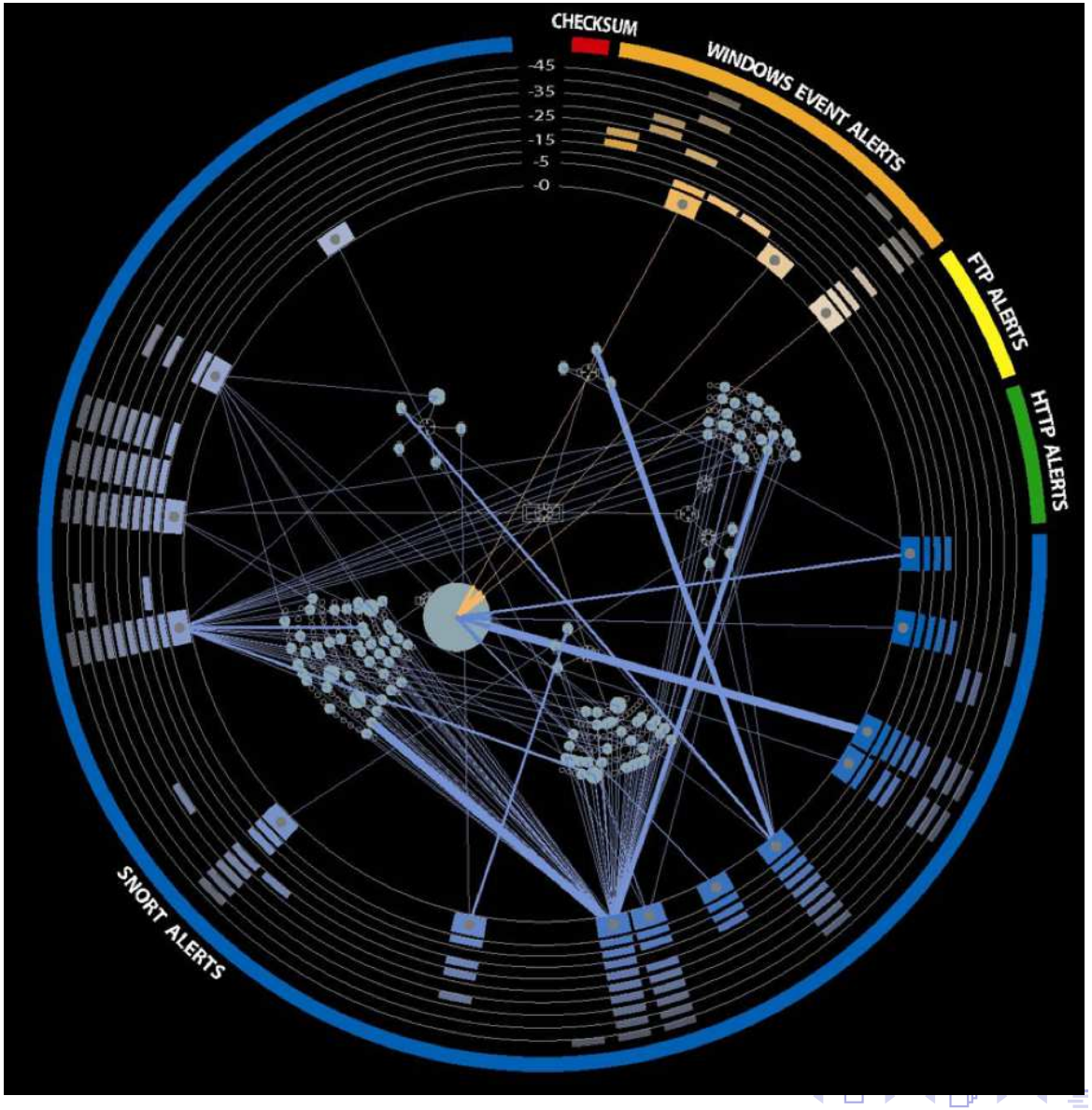
Port Scan: Processed Log Files (psad)

src:	dst:	chain:	intf:	tcp:	udp:	icmp:	dl:	alerts:	os_guess:
117.32.xxx.149	xx.22.zz.121	INPUT	eth0	1	0	0	2	2	-
118.167.xxx.219	xx.22.zz.121	INPUT	eth0	1	0	0	2	2	-
118.167.xxx.250	xx.22.zz.121	INPUT	eth0	1	0	0	2	2	-
118.167.xxx.5	xx.22.zz.121	INPUT	eth0	1	0	0	2	2	-
122.167.xx.11	xx.22.zz.121	INPUT	eth0	4642	0	0	4	50	-
122.167.xx.80	xx.22.zz.121	INPUT	eth0	0	11	0	1	2	-
123.134.xx.34	xx.22.zz.121	INPUT	eth0	20	0	0	2	9	-
125.161.xx.3	xx.22.zz.121	INPUT	eth0	0	9	0	1	4	-
125.67.xx.7	xx.22.zz.121	INPUT	eth0	1	0	0	2	2	-
190.159.xxx.220	xx.22.zz.121	INPUT	eth0	0	9	0	1	3	-
193.140.xxx.210	xx.22.zz.121	INPUT	eth0	0	10	0	1	2	-
202.xx.23x.196	xx.22.zz.121	INPUT	eth0	0	13	0	1	10	-
202.xx.2x8.197	xx.22.zz.121	INPUT	eth0	0	20	0	2	17	-
202.97.xxx.198	xx.22.zz.121	INPUT	eth0	0	17	0	2	12	-
202.97.xxx.199	xx.22.zz.121	INPUT	eth0	0	18	0	2	15	-
202.97.xxx.200	xx.22.zz.121	INPUT	eth0	0	17	0	2	14	-
202.97.xxx.201	xx.22.zz.121	INPUT	eth0	0	15	0	2	12	-
202.97.xxx.202	xx.22.zz.121	INPUT	eth0	0	21	0	2	16	-
203.xxx.128.65	xx.22.zz.121	INPUT	eth0	12	0	0	2	6	Windows XP/2000
211.90.xx.14	xx.22.zz.121	INPUT	eth0	1	0	0	2	2	-
213.163.xxx.9	xx.22.zz.121	INPUT	eth0	0	0	1	2	2	-
221.130.xxx.124	xx.22.zz.121	INPUT	eth0	0	35	0	2	31	-
221.206.xxx.10	xx.22.zz.121	INPUT	eth0	0	33	0	2	21	-
221.206.xxx.53	xx.22.zz.121	INPUT	eth0	0	33	0	2	27	-
221.206.xxx.54	xx.22.zz.121	INPUT	eth0	0	39	0	2	26	-
221.206.xxx.57	xx.22.zz.121	INPUT	eth0	0	33	0	2	19	-
60.222.xxx.146	xx.22.zz.121	INPUT	eth0	0	40	0	2	33	-
60.222.xxx.153	xx.22.zz.121	INPUT	eth0	0	14	0	1	11	-
60.222.xxx.154	xx.22.zz.121	INPUT	eth0	0	18	0	2	15	-

Port Scan: Visualization



Circular Visualization



Pre-Attentive Objects

1. Color

Pre-Attentive Objects

1. Color
2. Position

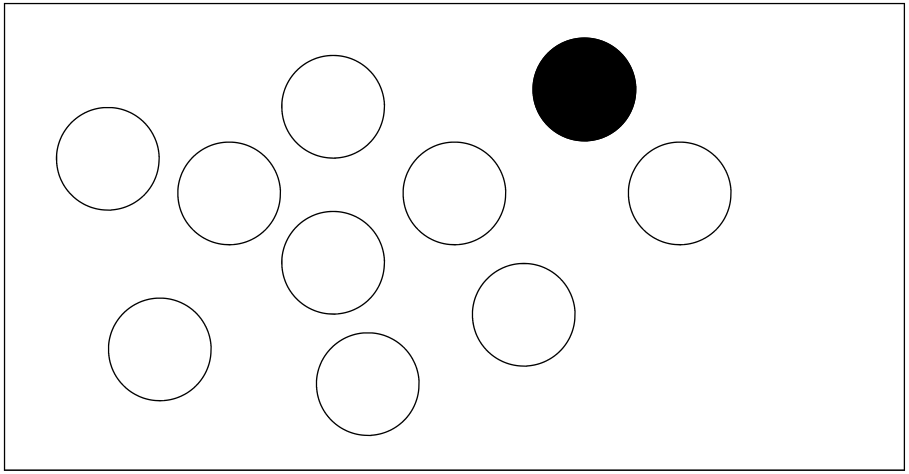
Pre-Attentive Objects

1. Color
2. Position
3. Form

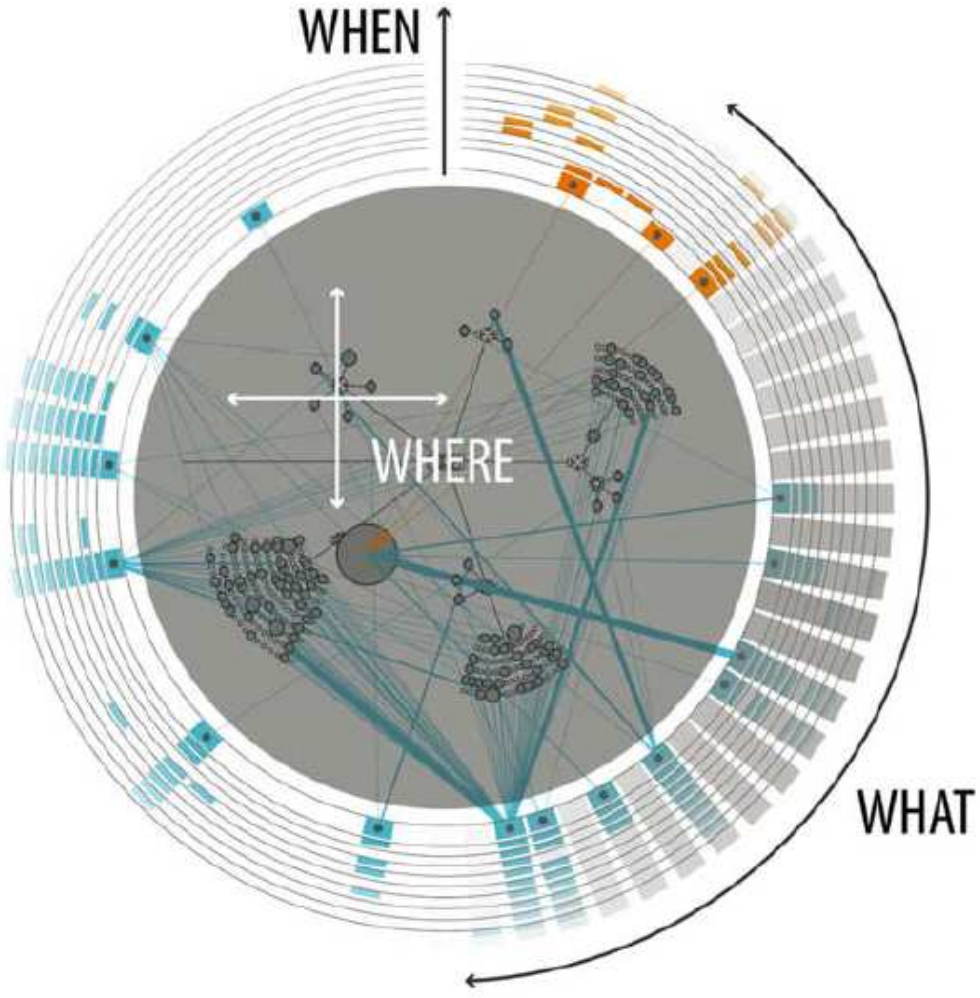
Pre-Attentive Objects

1. Color
2. Position
3. Form
4. Motion

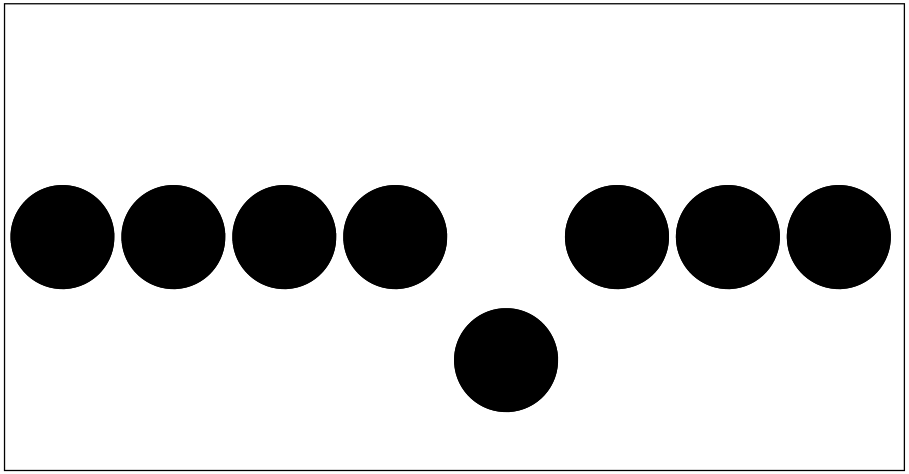
Pre-Attentive: Color



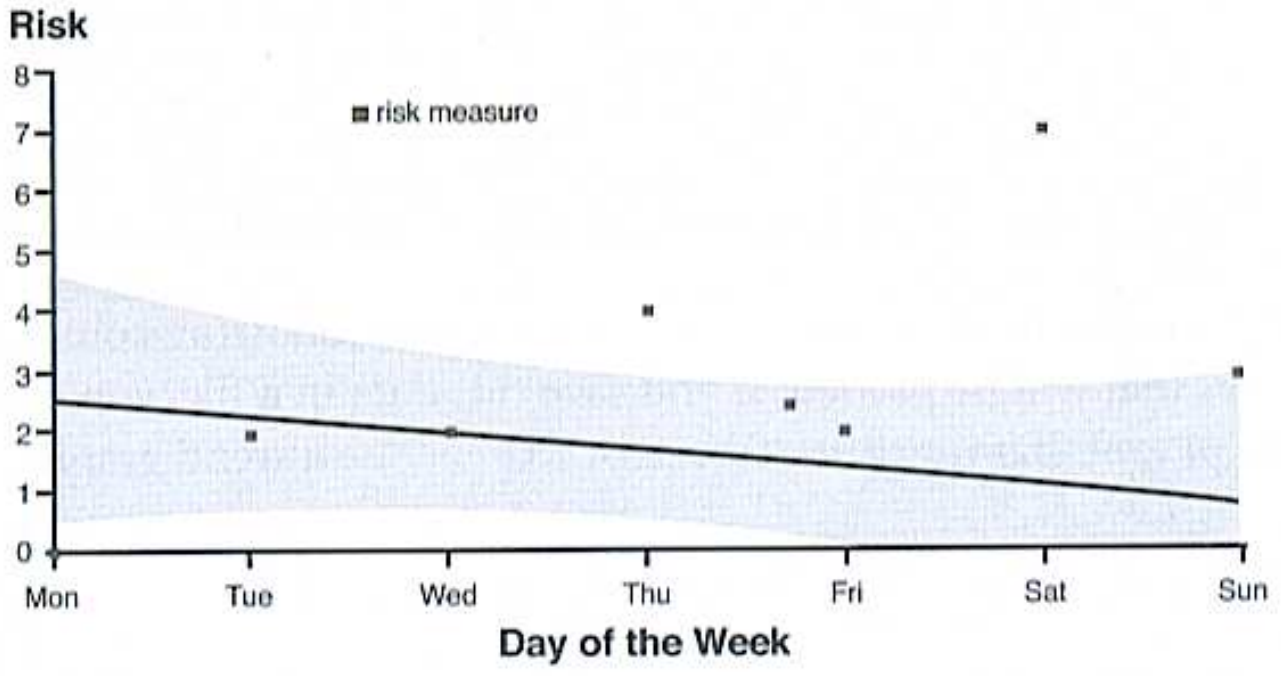
Visualization Applying Color



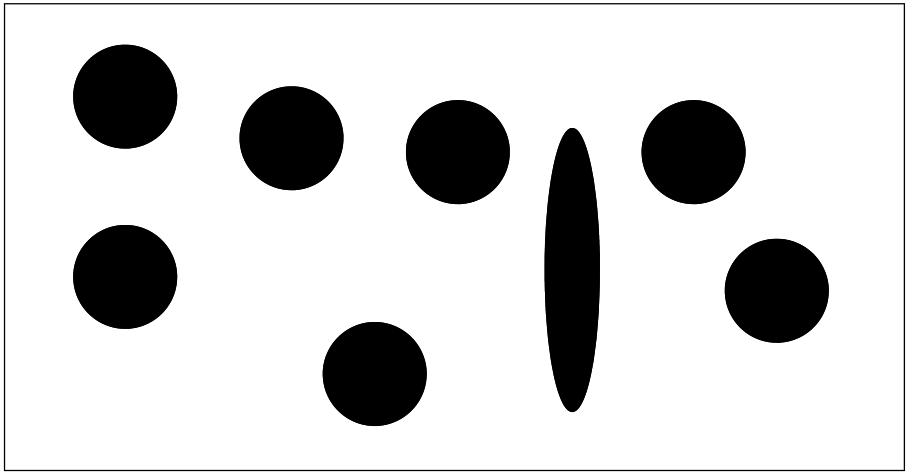
Pre-Attentive: Postion



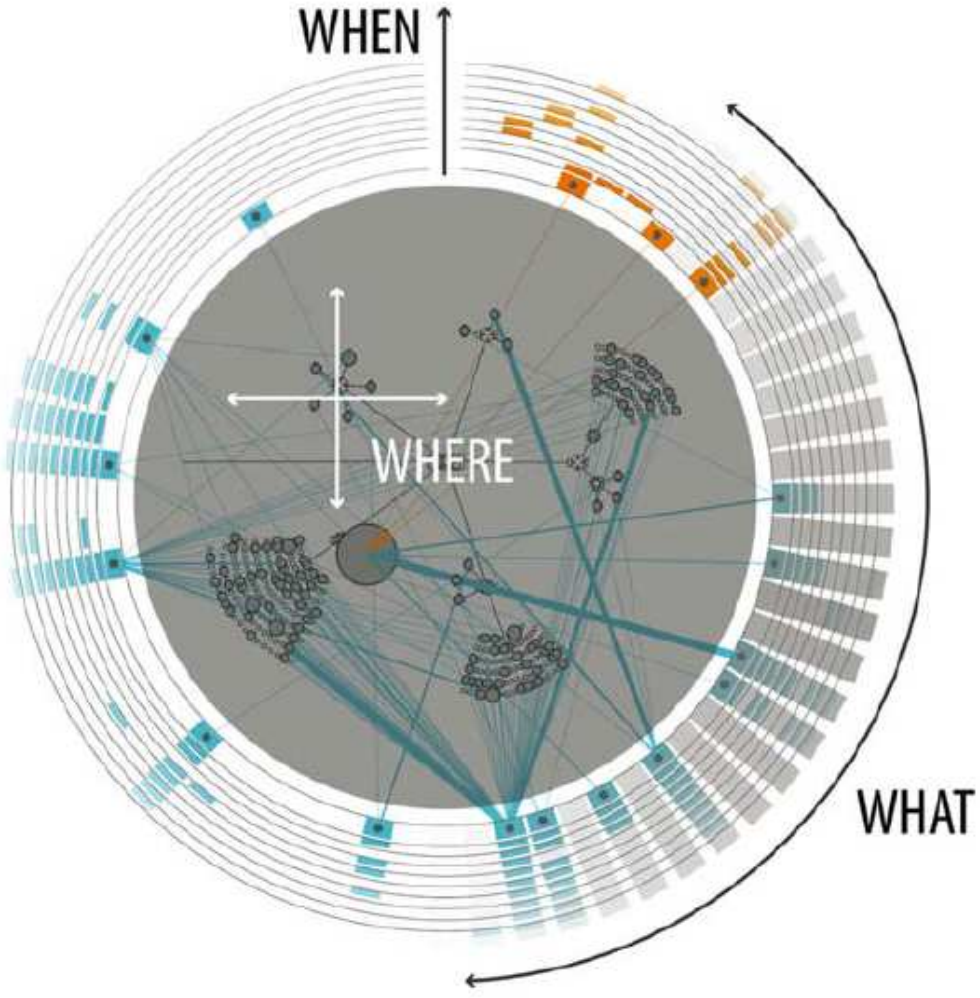
Visualization Applying Position



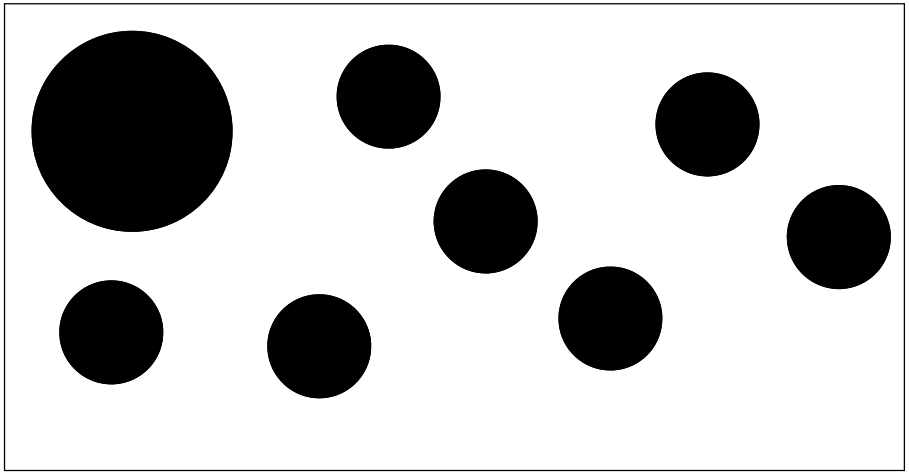
Pre-Attentive: Form - Shape



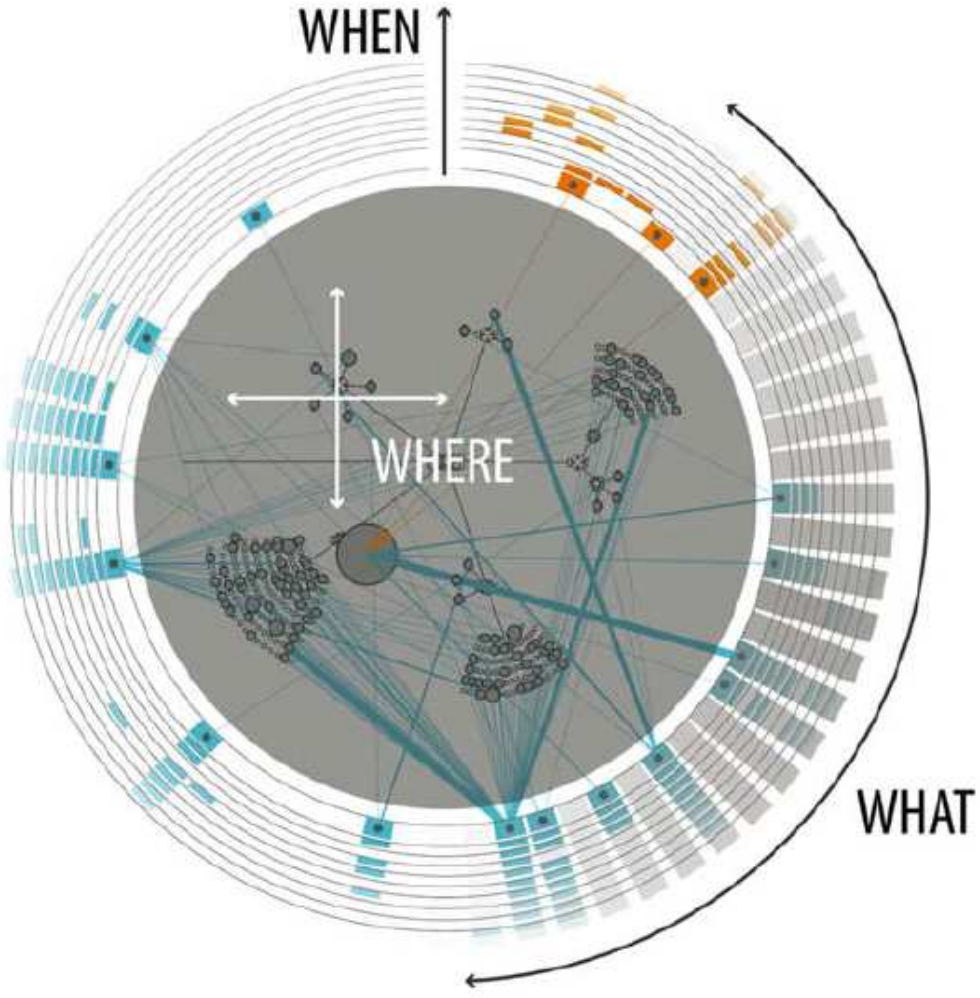
Visualization Applying Shape



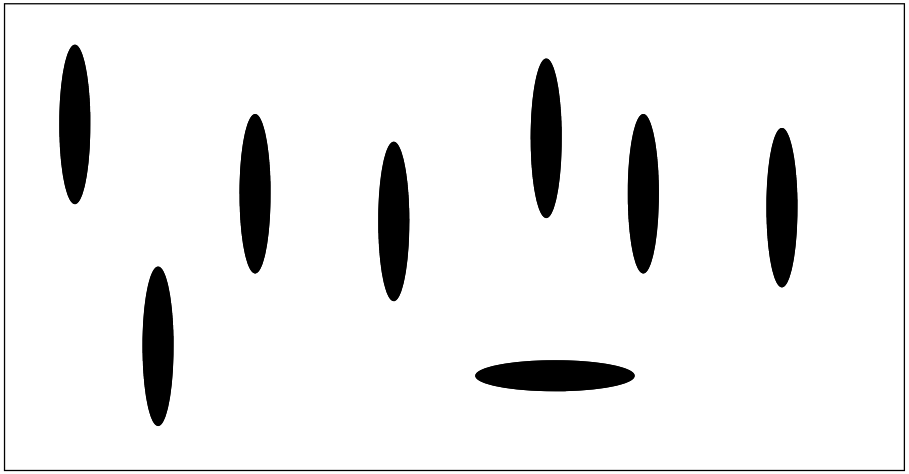
Pre-Attentive: Form - Size



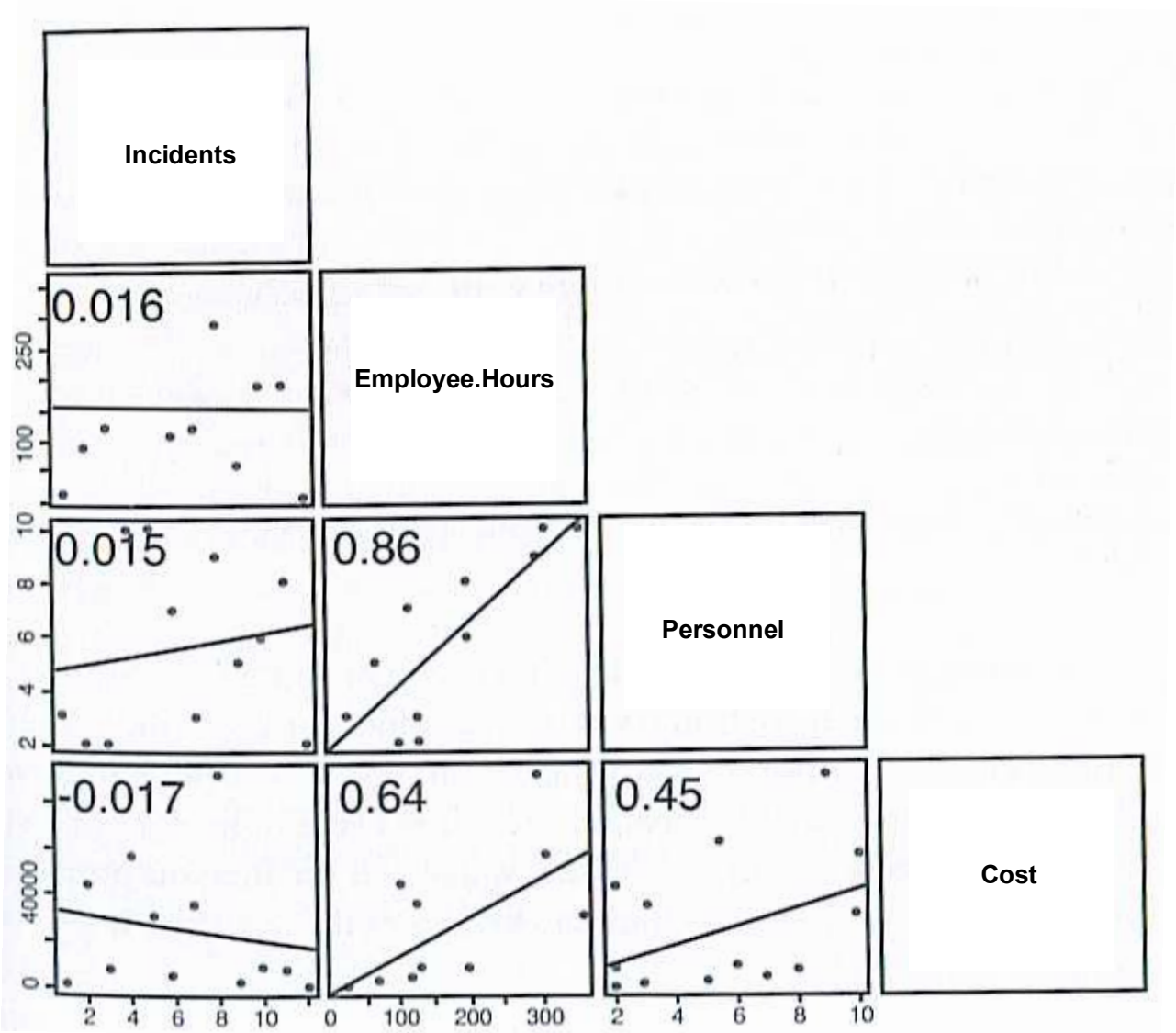
Visualization Applying Size



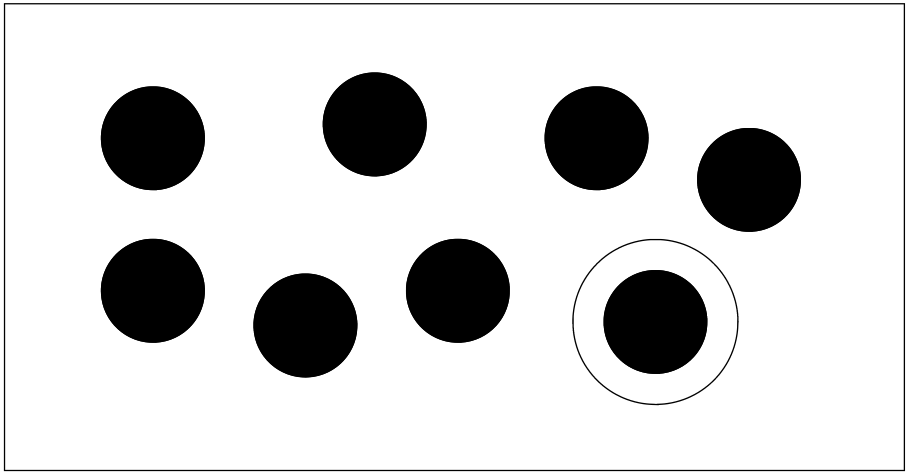
Pre-Attentive: Form - Orientation



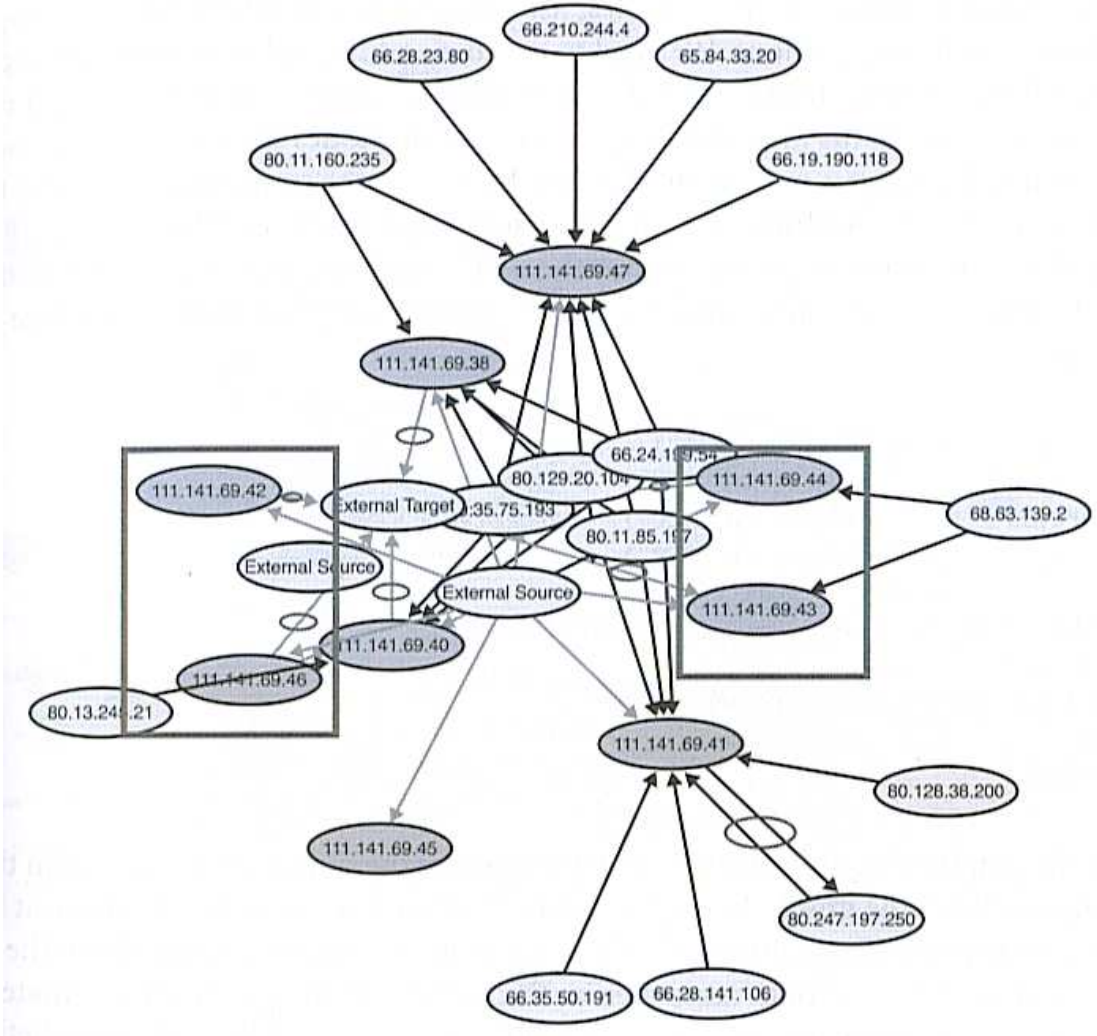
Visualization using Orientation



Pre-Attentive: Form - Enclosure



Visualization using Enclosure



Visualization Techniques

1. No serial parsing

Visualization Techniques

1. No serial parsing
2. Minimize the Number of Types Of Objects

Visualization Techniques

1. No serial parsing
2. Minimize the Number of Types Of Objects
3. Minimize Non-data Ink/Pixels

No Serial Parsing

30913646251849
50018364527489
40392726584019
18127365859202

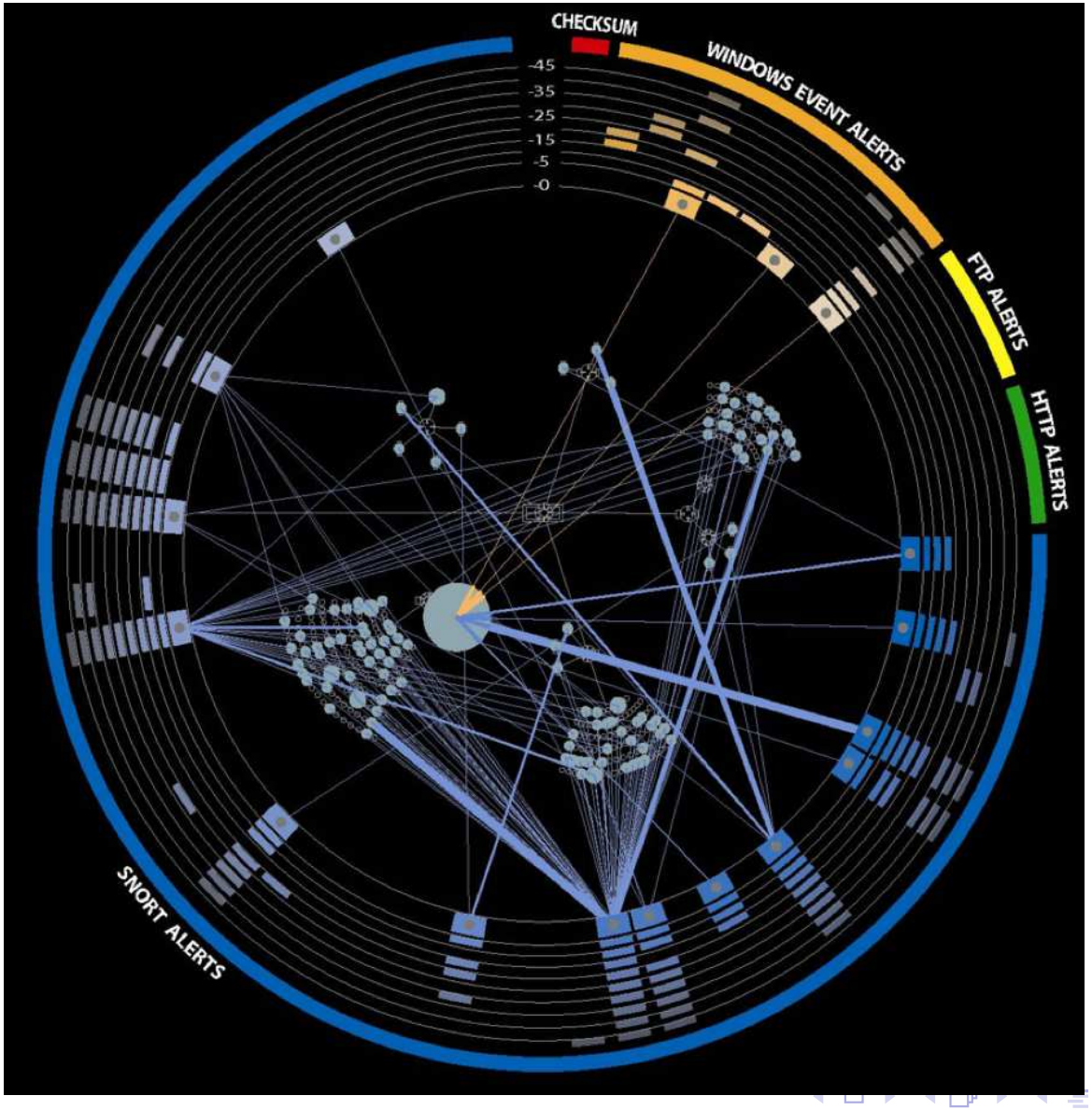
No Serial Parsing

30913646251849
50018364527489
40392726584019
18127365859202

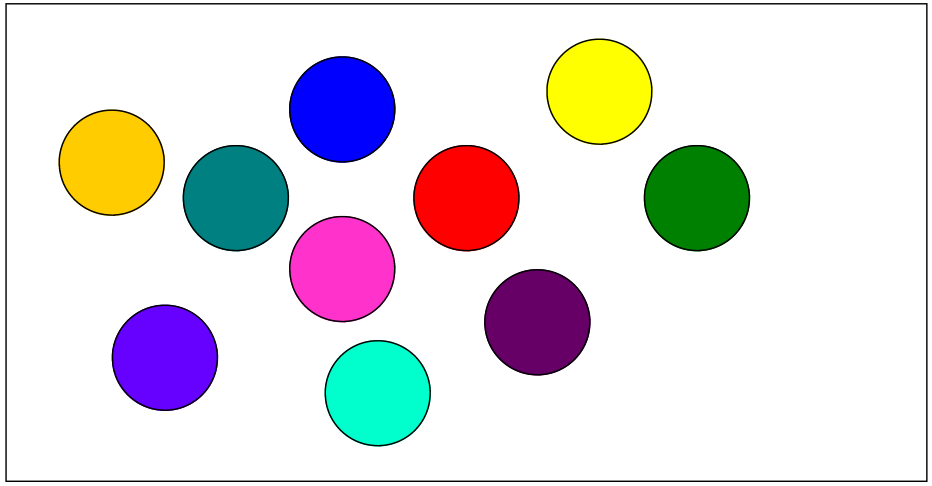
VS

30913646251849
50018364527489
40392726584019
18127365859202

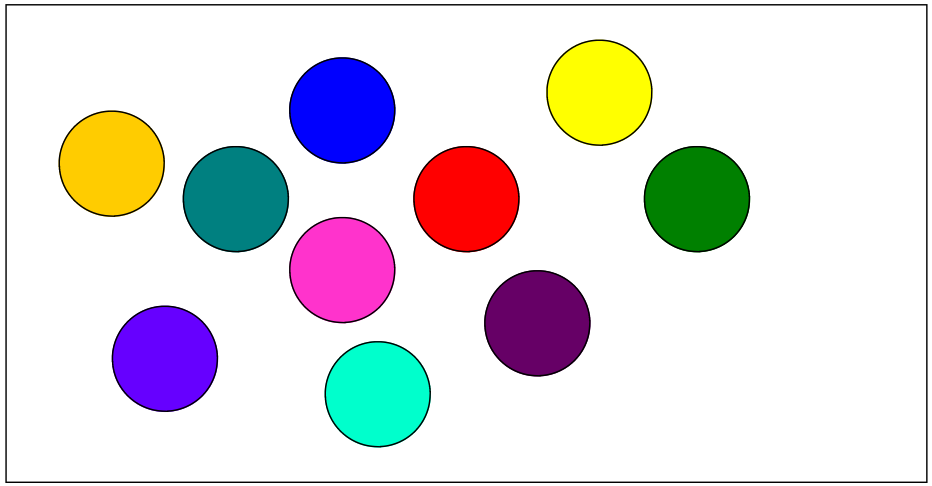
Visualization Applying No Serial Parsing



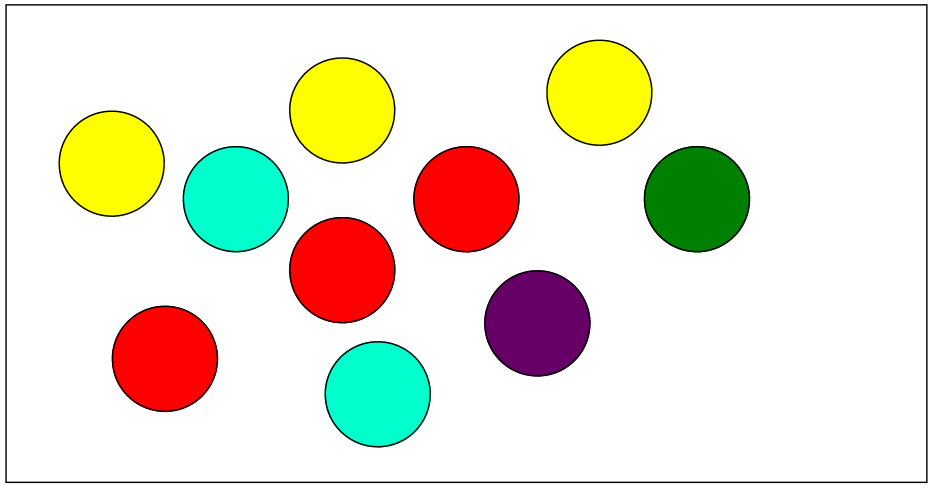
Minimize the Number of Types Of Objects



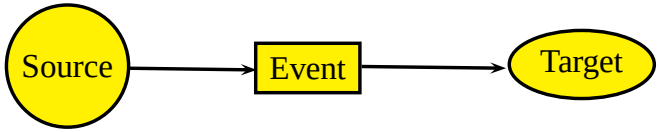
Minimize the Number of Types Of Objects



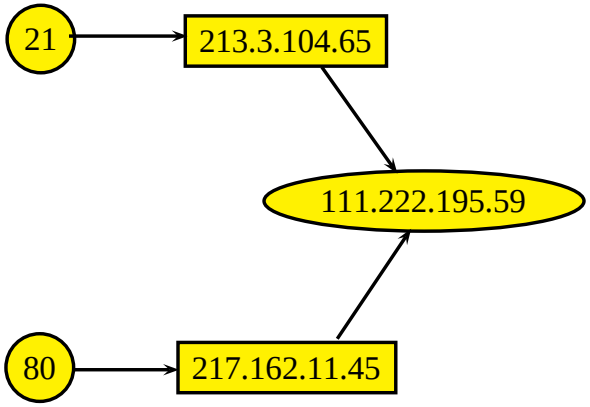
VS



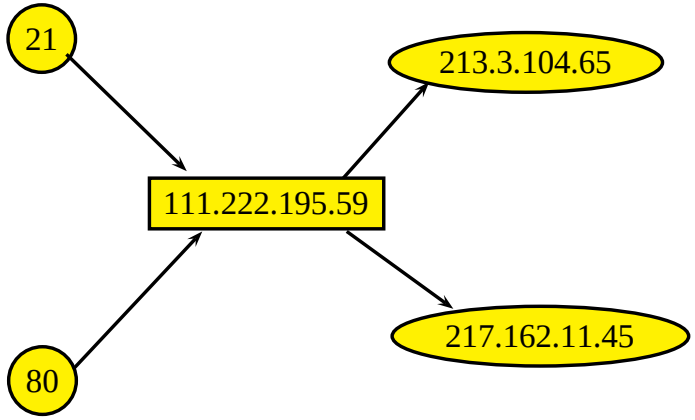
Visualization Applying Minimum Objects



(a) Link graph nomenclature.

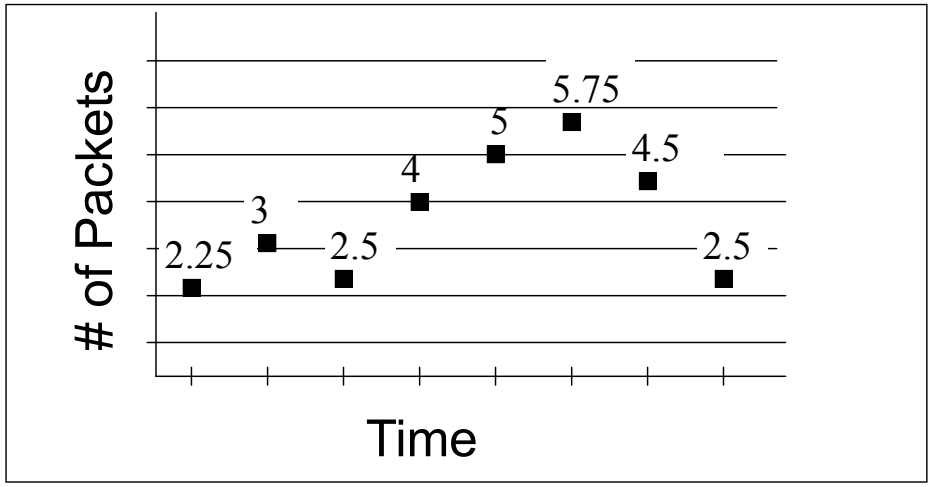


(b) Destination port, source address, and destination address.

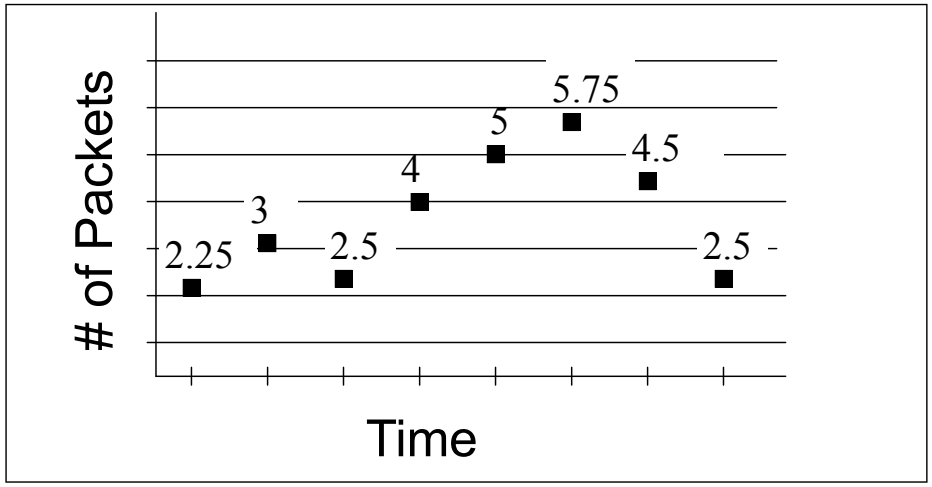


(c) Destination port, destination address, and source address.

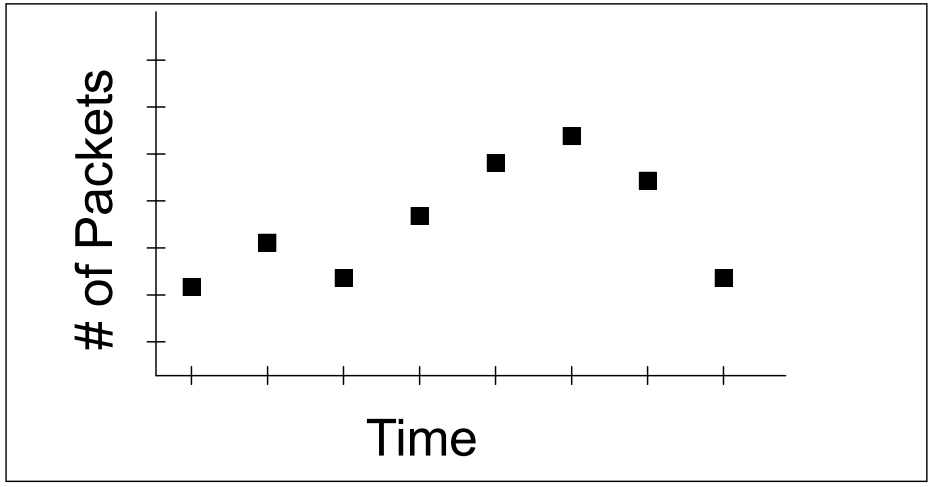
Minimize Non-data Ink/Pixels



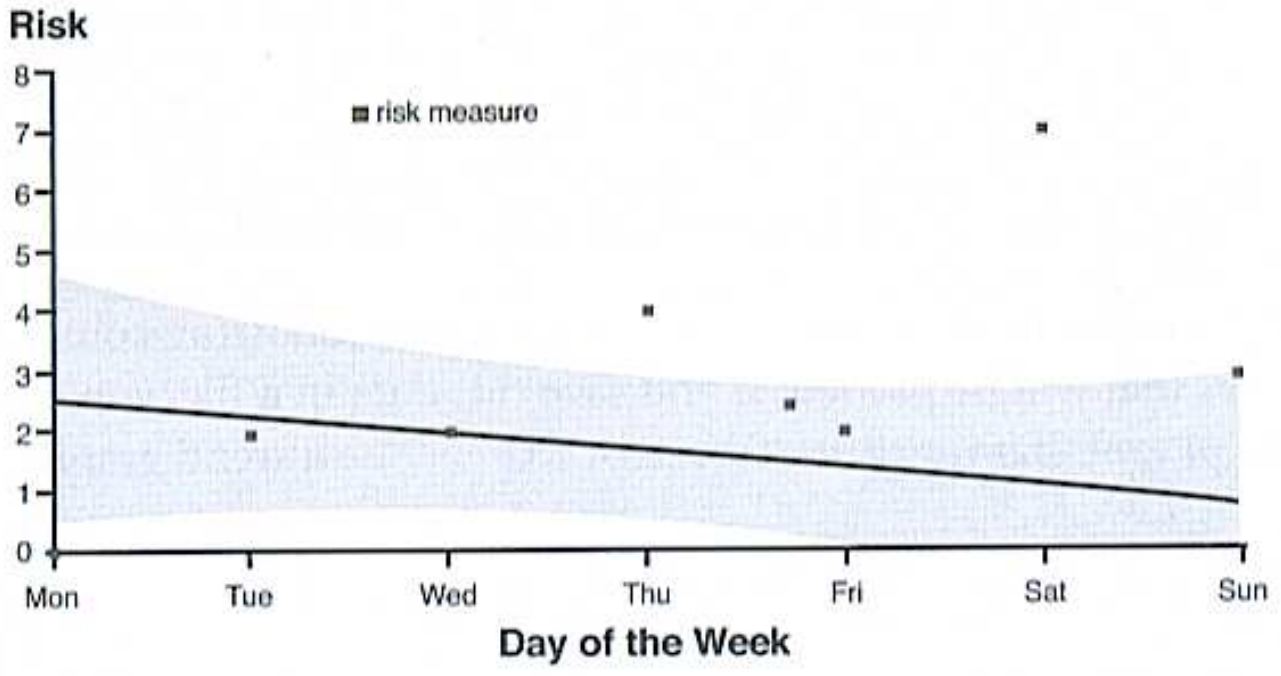
Minimize Non-data Ink/Pixels



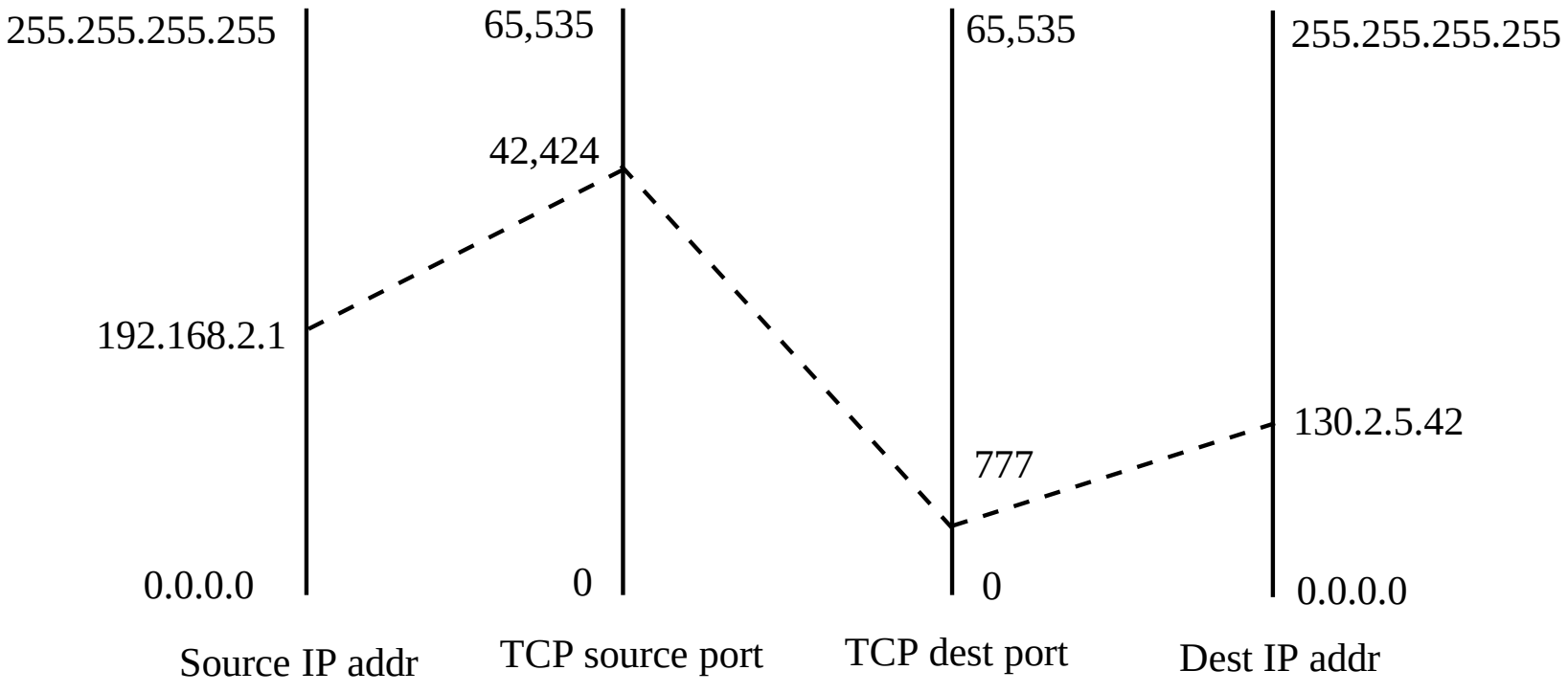
VS



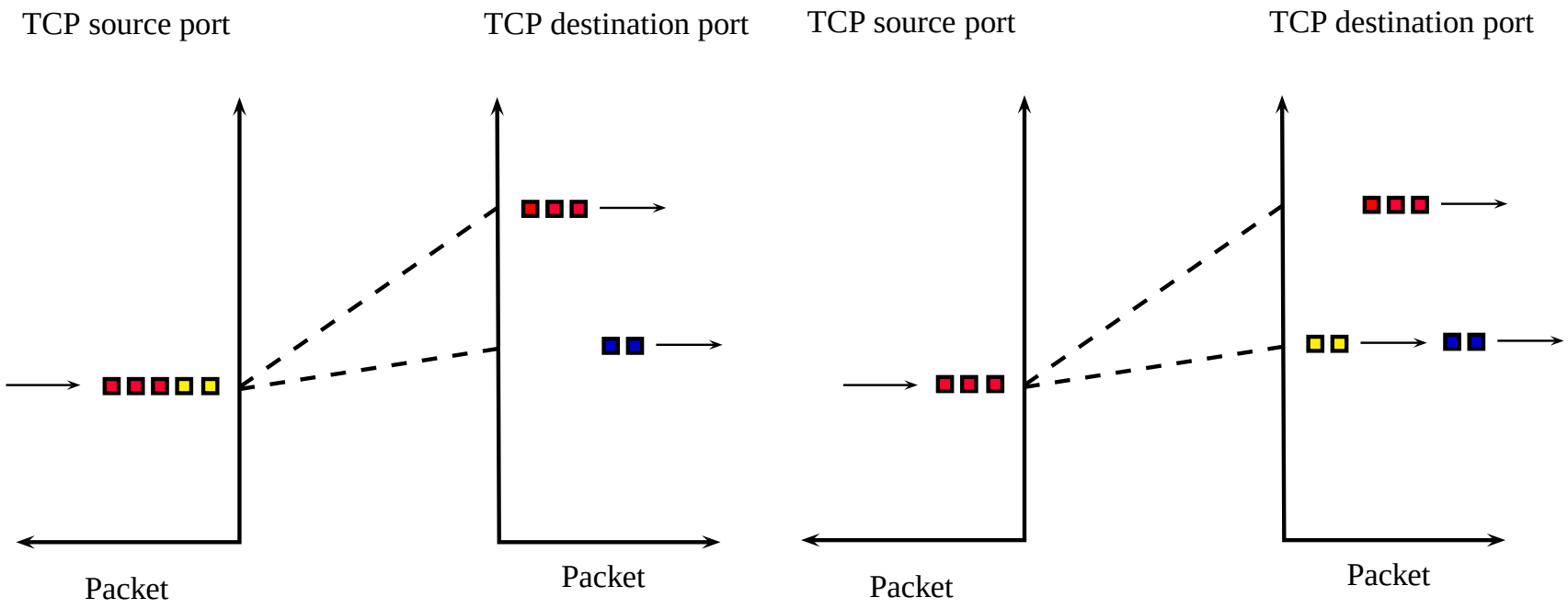
Visualization Applying Non-data Ink/Pixels



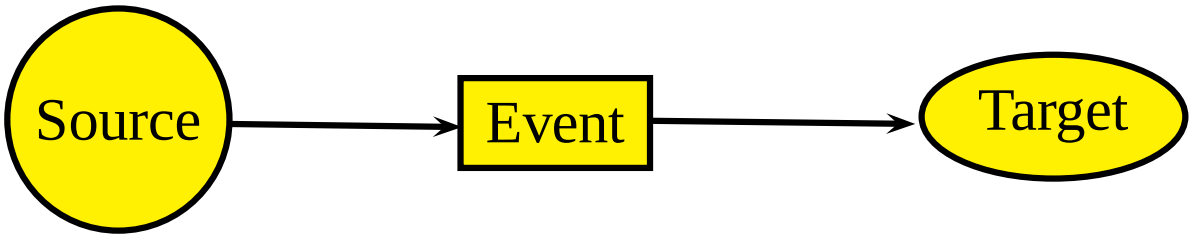
Parallel Plots



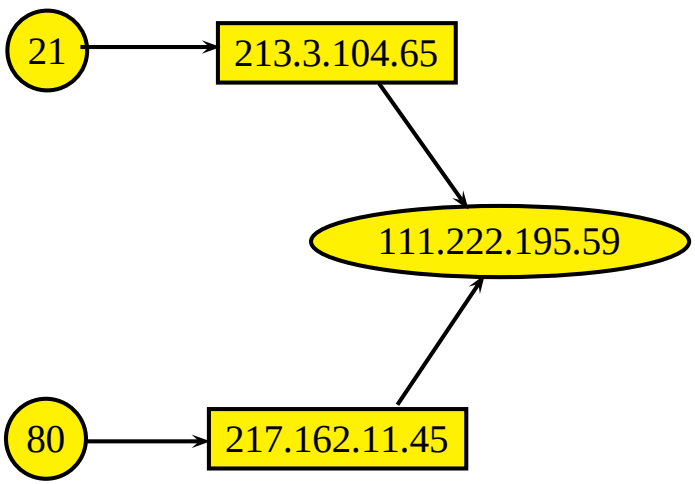
Animated Parallel Plots

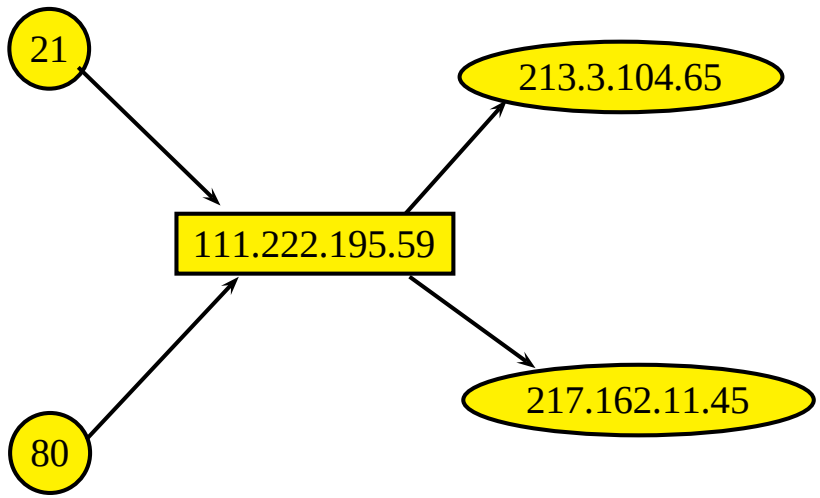


Link graphs: nomenclature



Link graphs: hidden information





Demo Network Visualization Tool

- Demo

References

[1] Robert Ball, Glenn A. Fink, and Chris North. Home-centric visualization of network traffic for security administration. In In VizSEC/DMSEC 04: Proceedings of the 2004 ACM workshop on Visualization and, pages 5564. ACM Press, 2004.

[2] Ryan Blue, Cody Dunne, Adam Fuchs, Kyle King, and Aaron Schulman. Visualizing real-time network resource usage. In Proceedings of the 5th international workshop on Visualization for Computer Security, VizSec 08, pages 119135, Berlin, Heidelberg, 2008. Springer-Verlag.

[3] Bill Cheswick, Hal Burch, and Steve Branigan. Mapping and visualizing the internet. In Proceedings of the annual conference on USENIX Annual Technical Conference, ATEC 00, pages 11, Berkeley, CA, USA, 2000. USENIX Association.

[4] Greg Conti. Security Data Visualization: Graphical Techniques for Network Analysis. No Starch Press, 2007.

[5] Anita D. DAmico and K. Whitley. The real work of computer network defense analysts. In Goodall et al. [8], pages 1937.

[6] Stefano Foresti, Jim Agutter, Yarden Livnat, Shaun Moon, and Robert Erbacher. Visual correlation of network alerts. In IEEE Computer Graphics and Applications, pages 4859. IEEE, 2006.

[7] J. R. Goodall. Introduction to visualization for computer security. In John R. Goodall, Gregory Conti, and Kwan-Liu Ma, editors, VizSEC 2007, Mathematics and Visualization, pages 117. Springer Berlin Heidelberg, 2008. 10.1007/978-3-540-78243-8 1.

[8] John R. Goodall, Gregory J. Conti, and Kwan-Liu Ma, editors. VizSEC 2007, Proceedings of the Workshop on Visualization for Computer Security, Sacramento, California, USA, October 29, 2007, Mathematics and Visualization. Springer, 2008.

[9] Ivan Herman, Guy Melancon, and M. Scott Marshall. Graph visualization and navigation in information visualization: A survey. IEEE Transactions on Visualization and Computer Graphics, 6:2443, January 2000.

[10] Noah Iliinsky Julie Steele. Beautiful Visualization. OReilly Media, Inc., 2010.

[11] Noah Iliinsky Julie Steele. Designing Data Visualizations. OReilly Media, Inc., 2011.

[12] A. Komlodi, P. Rheingans, Utkarsha Ayachit, J.R. Goodall, and Amit Joshi. A user-centered look at glyph-based security visualization. In Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on, pages 21 28, oct. 2005.

References cont.

[13] Kiran Lakkaraju, William Yurcik, and Adam J. Lee. Nvisionip: netflow visualizations of system state for security situational awareness. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, VizSEC/DMSEC 04, pages 6572, New York, NY, USA, 2004. ACM.

[14] C.P. Lee, J. Trost, N. Gibbs, Raheem Beyah, and J.A. Copeland. Visual firewall: real-time network security monitor. In Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on, pages 129 136, oct. 2005.

[15] Yarden Livnat, Jim Agutter, Shaun Moon, Robert F. Erbacher, and Stefano Foresti. A vi- sualization paradigm for network intrusion detection. In In Proceedings of the 2005 IEEE Workshop on Information Assurance And Security, pages 9299. IEEE, 2005.

[16] Raffael Marty. Applied Security Visualization. Addison-Wesley Professional, 2008.

[17] Jonathan McPherson, Kwan-Liu Ma, Paul Krystosk, Tony Bartoletti, and Marvin Christensen. Portvis: a tool for port-based detection of security events. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, VizSEC/DMSEC 04, pages 7381, New York, NY, USA, 2004. ACM.

[18] Toby Segaran. Programming Collective Intelligence. OReilly Media, Inc., 2007.

[19] Colin Ware. Information Visualization: Perception for Design. Morgan Kaufmann Publishers, 2004.

[20] Christopher D. Wickens, Diane L. Sandry, and Michael Vidulich. Compatibility and resource competition between modalities of input, central processing, and output. Human Factors: The Journal of the Human Factors and Ergonomics Society, 25(2):227248, 1983.