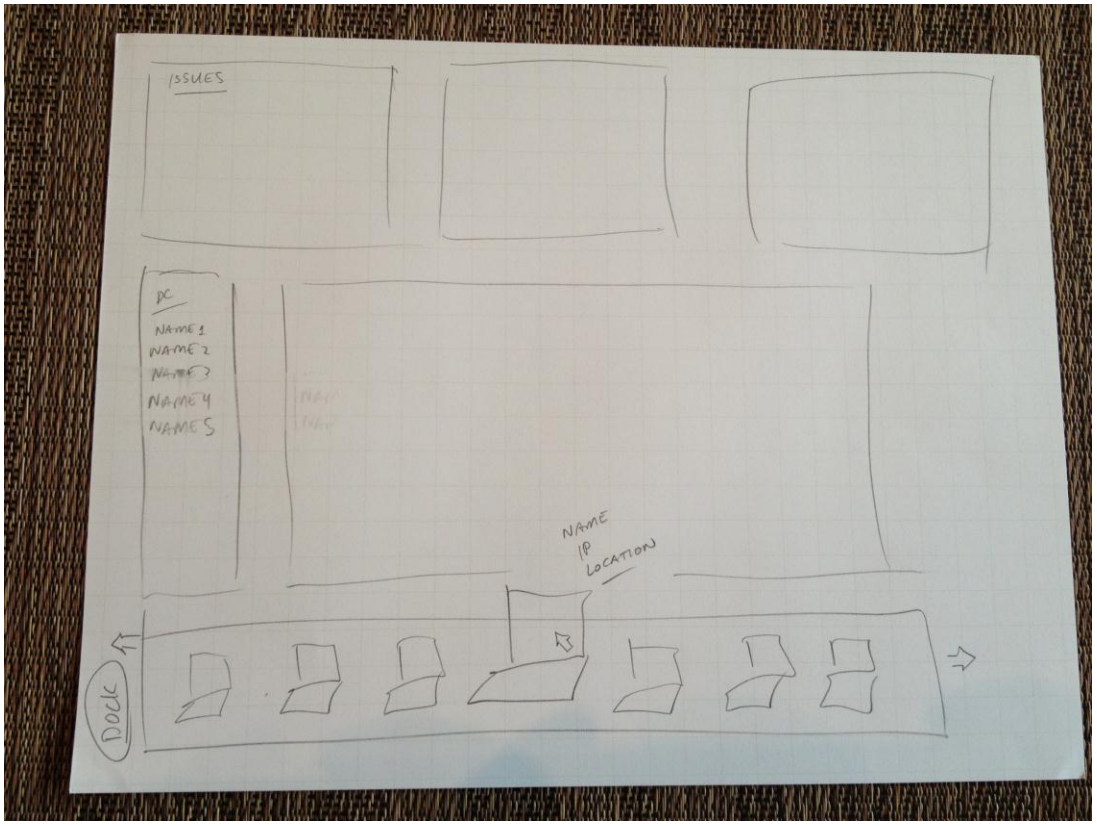
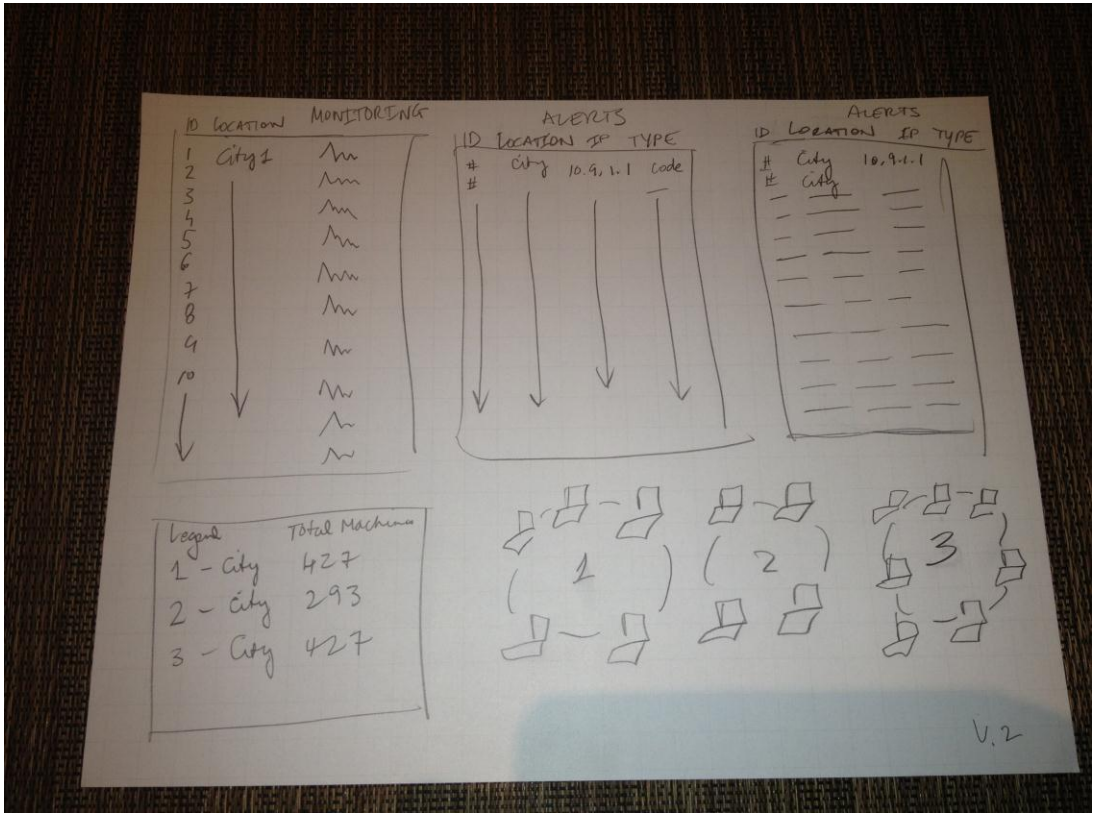


Description

The original design was a cross between a dock at the bottom of the dashboard and a handful of 'heads-up' displays. When a user would scroll over an 'Issue' on any of the heads-up displays, the name of the Data Center (DC) would be displayed. Users could then drill down into each data center. When a user would drill down into the Data Center, machines and devices in the Data Center would be displayed across the bottom of the screen. The dock display would allow the user to identify the Name, IP Address, and Location (by Zone) of the machine by hovering over the computer icon or by using the left and right arrows located at the sides of the dock.

Notes

1. This design had several flaws to include but not limited to:
    a. The area in the 'dock' would never scale to meet multiple cities. The graphics used for the computers were taking up too much real estate. Discussions were conducted about using the arrow buttons on the left and ride sides of the dock; however, the team agreed that this would still take up too much real estate on the dashboard.
    b. The layout was not working for as much information that would need to be shared.
2. For the next iteration of the dashboard, the team agreed to have limited graphics and icons displayed to conserve space.



Description

The next iteration of the dashboard would require a move in a different direction in order to meet all the requirements.

First, everything was going to be text based and icons or images were going to be greatly reduced. Secondly, the team wanted to incorporate sparklines in order to quickly identify patterns and trends.

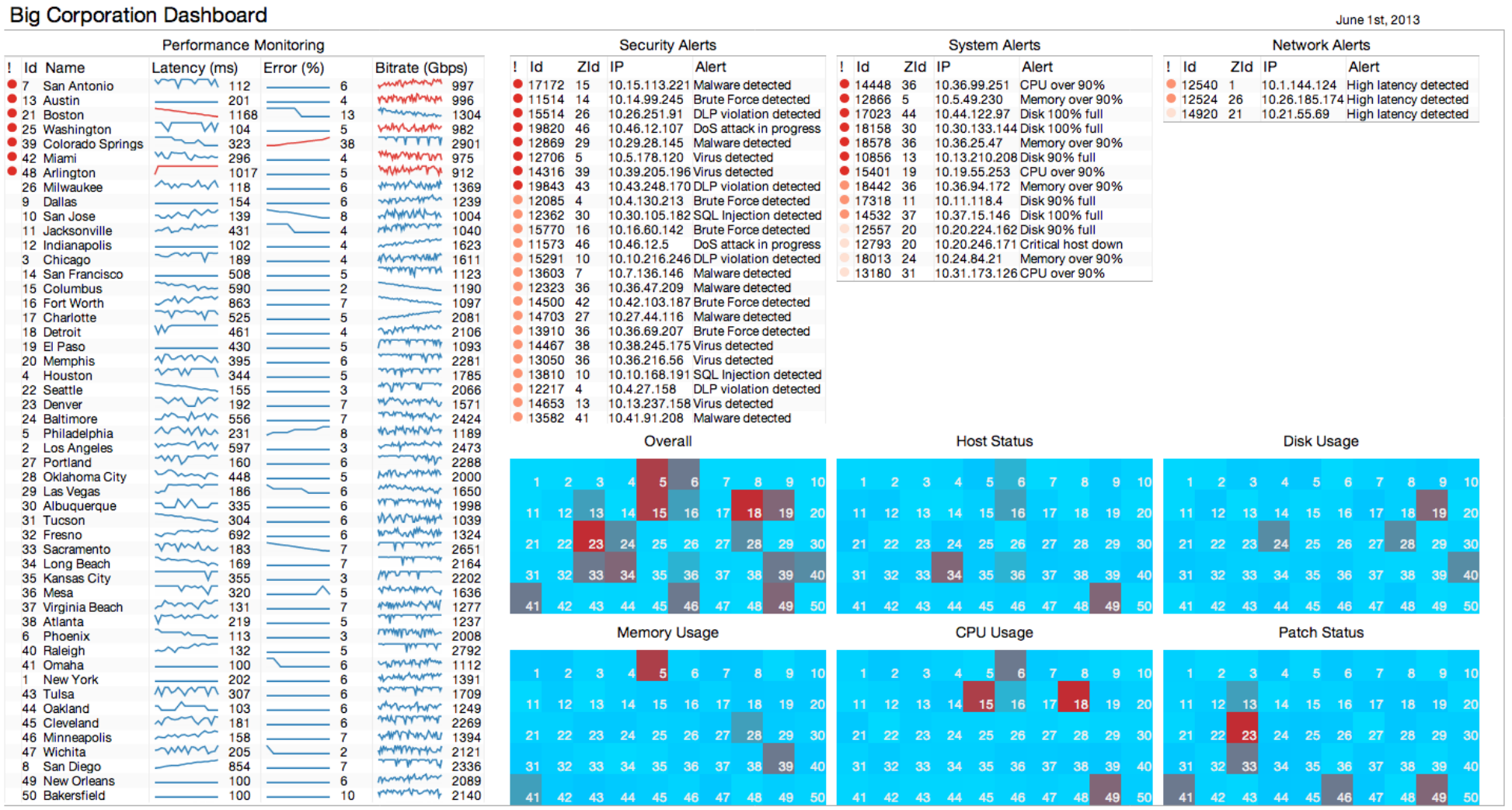
Another evolution to the dashboard was creating the types of zones that would be incorporated into the display. Zones are an area that would allow a user to quickly identify how a machine in a specific zone was performing. Trending data for a machine in a zone would allow a user to identify:

1. Physical location by city
2. Performance of the location
3. Errors

Security, System, and Network Alerts were also added to the dashboard.

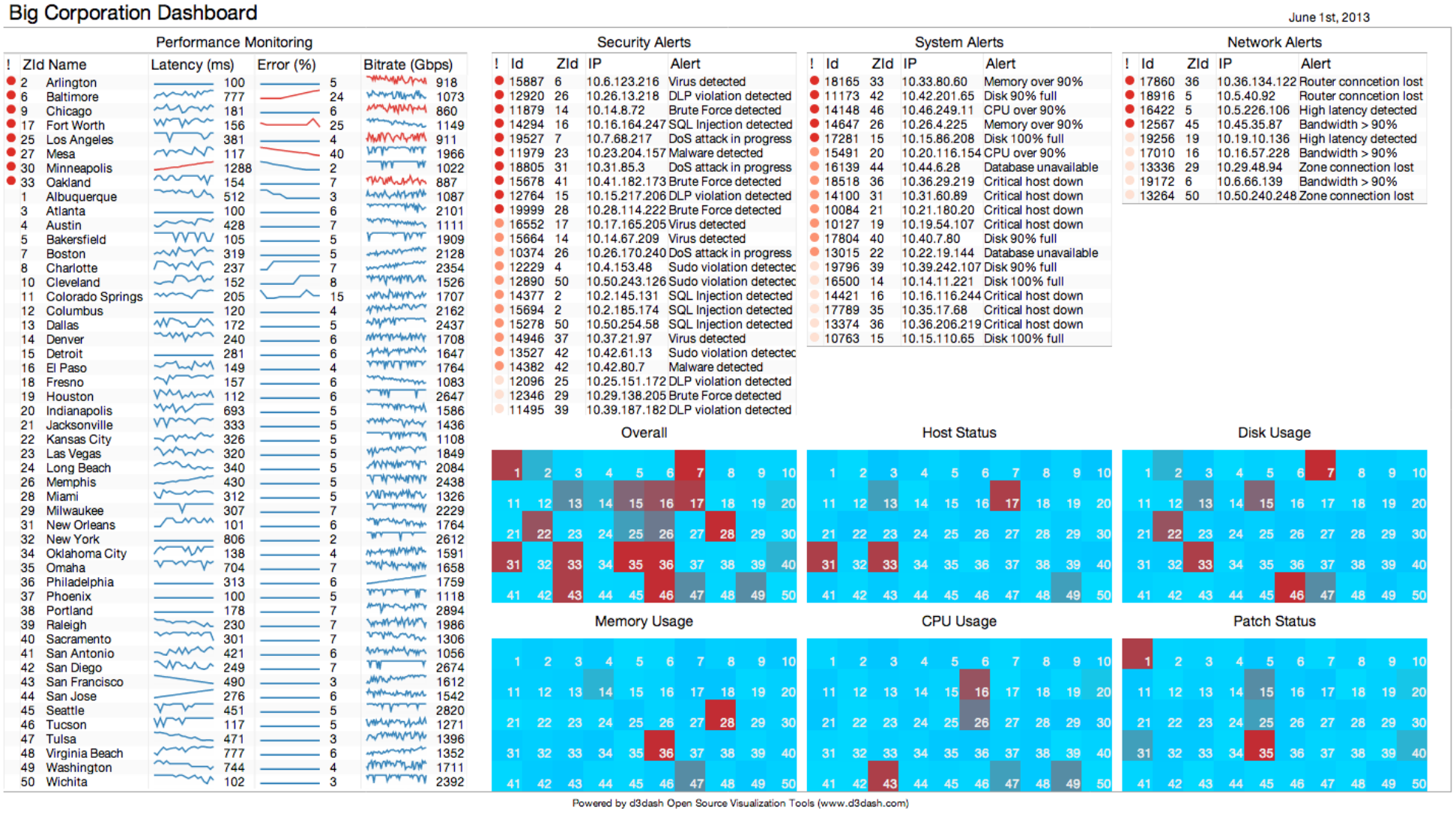
Notes

1. Discussions about what to do with the white space on the bottom right occurred since there were a couple options – either a network map or a representation of the Zones with associated health status or a combination of the two would need to be incorporated.
2. The team discussed using Andy Hoernecke's Open Source Project, D3 Dash to generate future iterations of Dashboards for this project.



Notes

1. The team wanted to create the dashboard in order to start visualizing the layout, which worked out well for creating the first review.
2. The areas that were created for this review were: Performance Monitoring, Security Alerts, System Alerts, Network Alerts, and a Heatmap
3. Some issues identified with this revision were that the cities that were listed were only US-based. Another issue was that information was truncated under the Security Alerts.
4. Visual display colors were added to the 'Alerts' by a slow red to orange change so that individuals could analyze information by a quick scan for a change in color.



!	ZId	Name	Latency (ms)	Error (%)	Bitrate (Gbps)
●	2	Arlington	100	5	918
●	6	Baltimore	777	24	1073
●	9	Chicago	181	6	860
●	17	Fort Worth	156	25	1149
●	25	Los Angeles	381	4	911
●	27	Mesa	117	40	1966
●	30	Minneapolis	1288	2	1022
●	33	Oakland	154	7	887
	1	Albuquerque	512	3	1087
	3	Atlanta	100	6	2101
	4	Austin	428	7	1111
	5	Bakersfield	105	5	1909
	7	Boston	319	5	2128
	8	Charlotte	237	7	2354
	10	Cleveland	152	8	1526
	11	Colorado Springs	205	15	1707
	12	Columbus	120	4	2162
	13	Dallas	172	5	2437
	14	Denver	240	6	1708
	15	Detroit	281	6	1647
	16	El Paso	149	4	1764
	18	Fresno	157	6	1083
	19	Houston	112	6	2647
	20	Indianapolis	693	5	1586
	21	Jacksonville	333	5	1436
	22	Kansas City	326	5	1108
	23	Las Vegas	320	5	1849
	24	Long Beach	340	5	2084
	26	Memphis	430	5	2438
	28	Miami	312	5	1326
	29	Milwaukee	307	7	2229
	31	New Orleans	101	6	1764
	32	New York	806	2	2612
	34	Oklahoma City	138	4	1591
	35	Omaha	704	7	1658
	36	Philadelphia	313	6	1759
	37	Phoenix	100	5	1118
	38	Portland	178	7	2894
	39	Raleigh	230	7	1986
	40	Sacramento	301	7	1306
	41	San Antonio	421	6	1056
	42	San Diego	249	7	2674
	43	San Francisco	490	3	1612
	44	San Jose	276	6	1542
	45	Seattle	451	5	2820
	46	Tucson	117	5	1271
	47	Tulsa	471	3	1396
	48	Virginia Beach	777	6	1352
	49	Washington	744	4	1711
	50	Wichita	102	3	2392

!	Id	ZId	IP	Alert
●	15887	6	10.6.123.216	Virus detected
●	12920	26	10.26.13.218	DLP violation detected
●	11879	14	10.14.8.72	Brute Force detected
●	14294	16	10.16.164.247	SQL Injection detected
●	19527	7	10.7.68.217	DoS attack in progress
●	11979	23	10.23.204.157	Malware detected
●	18805	31	10.31.85.3	DoS attack in progress
●	15678	41	10.41.182.173	Brute Force detected
●	12764	15	10.15.217.206	DLP violation detected
●	19999	28	10.28.114.222	Brute Force detected
●	16552	17	10.17.165.205	Virus detected
●	15664	14	10.14.67.209	Virus detected
●	10374	26	10.26.170.240	DoS attack in progress
●	12229	4	10.4.153.48	Sudo violation detected
●	12890	50	10.50.243.126	Sudo violation detected
●	14377	2	10.2.145.131	SQL Injection detected
●	15694	2	10.2.185.174	SQL Injection detected
●	15278	50	10.50.254.58	SQL Injection detected
●	14946	37	10.37.21.97	Virus detected
●	13527	42	10.42.61.13	Sudo violation detected
●	14382	42	10.42.80.7	Malware detected
	12096	25	10.25.151.172	DLP violation detected
	12346	29	10.29.138.205	Brute Force detected
	11495	39	10.39.187.182	DLP violation detected

!	Id	ZId	IP	Alert
●	18165	33	10.33.80.60	Memory over 90%
●	11173	42	10.42.201.65	Disk 90% full
●	14148	46	10.46.249.11	CPU over 90%
●	14647	26	10.26.4.225	Memory over 90%
●	17281	15	10.15.86.208	Disk 100% full
●	15491	20	10.20.116.154	CPU over 90%
●	16139	44	10.44.6.28	Database unavailable
●	18518	36	10.36.29.219	Critical host down
●	14100	31	10.31.60.89	Critical host down
●	10084	21	10.21.180.20	Critical host down
●	10127	19	10.19.54.107	Critical host down
●	17804	40	10.40.7.80	Disk 90% full
●	13015	22	10.22.19.144	Database unavailable
	19796	39	10.39.242.107	Disk 90% full
	16500	14	10.14.11.221	Disk 100% full
	14421	16	10.16.116.244	Critical host down
	17789	35	10.35.17.68	Critical host down
	13374	36	10.36.206.219	Critical host down
	10763	15	10.15.110.65	Disk 100% full

!	Id	ZId	IP	Alert
●	17860	36	10.36.134.122	Router conncetion lost
●	18916	5	10.5.40.92	Router conncetion lost
●	16422	5	10.5.226.106	High latency detected
●	12567	45	10.45.35.87	Bandwidth > 90%
	19256	19	10.19.10.136	High latency detected
	17010	16	10.16.57.228	Bandwidth > 90%
	13336	29	10.29.48.94	Zone connection lost
	19172	6	10.6.66.139	Bandwidth > 90%
	13264	50	10.50.240.248	Zone connection lost

Notes

1. This version of the alert dashboard mock-up were put in numeric order by ZoneID (ZID) and alphabetical order by city.
2. The issue with the cities only being in the US was still noted and would be addressed in a future mock-up of the design.
3. One item we struggled with was how to make items visually 'sortable'. We discussed having items with an underline call out; however, this presented issues with potential clutter on the dashboard.
4. The team discussed the need for adding a date and/or time stamp on the dashboard.
5. Another discussion that surfaced was to have a graphical representation to aid in "showing connections". Large networks with lots of nodes will be displayed when a user clicks through any of the respective areas.
6. Modifications to the Security, System and Network Alerts columns could show connections, but that may clutter the display.

Performance Monitoring Matrix

Legend: Latency (ms) - Error (%) - Bitrate (Gbps)	**Headquarters**	**Austin**	**Paris**	**New York**	**Dallas**	**Chicago**	**Sydney**	**Toronto**
Headquarters	203 - 9 - 983	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002
Austin	105 - 5 - 1002	203 - 9 - 983	105 - 5 - 1002	105 - 24 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002
Paris	105 - 5 - 1002	105 - 5 - 1002	203 - 9 - 983	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002
New York	105 - 5 - 1002	105 - 12 - 1002	105 - 5 - 1002	203 - 9 - 983	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002
Dallas	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	203 - 9 - 983	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002
Chicago	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	203 - 9 - 983	2000 - 5 - 1002	105 - 5 - 1002
Sydney	105 - 5 - 1002	105 - 5 - 50	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	203 - 9 - 983	105 - 5 - 1002
Toronto	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	105 - 5 - 1002	203 - 9 - 983

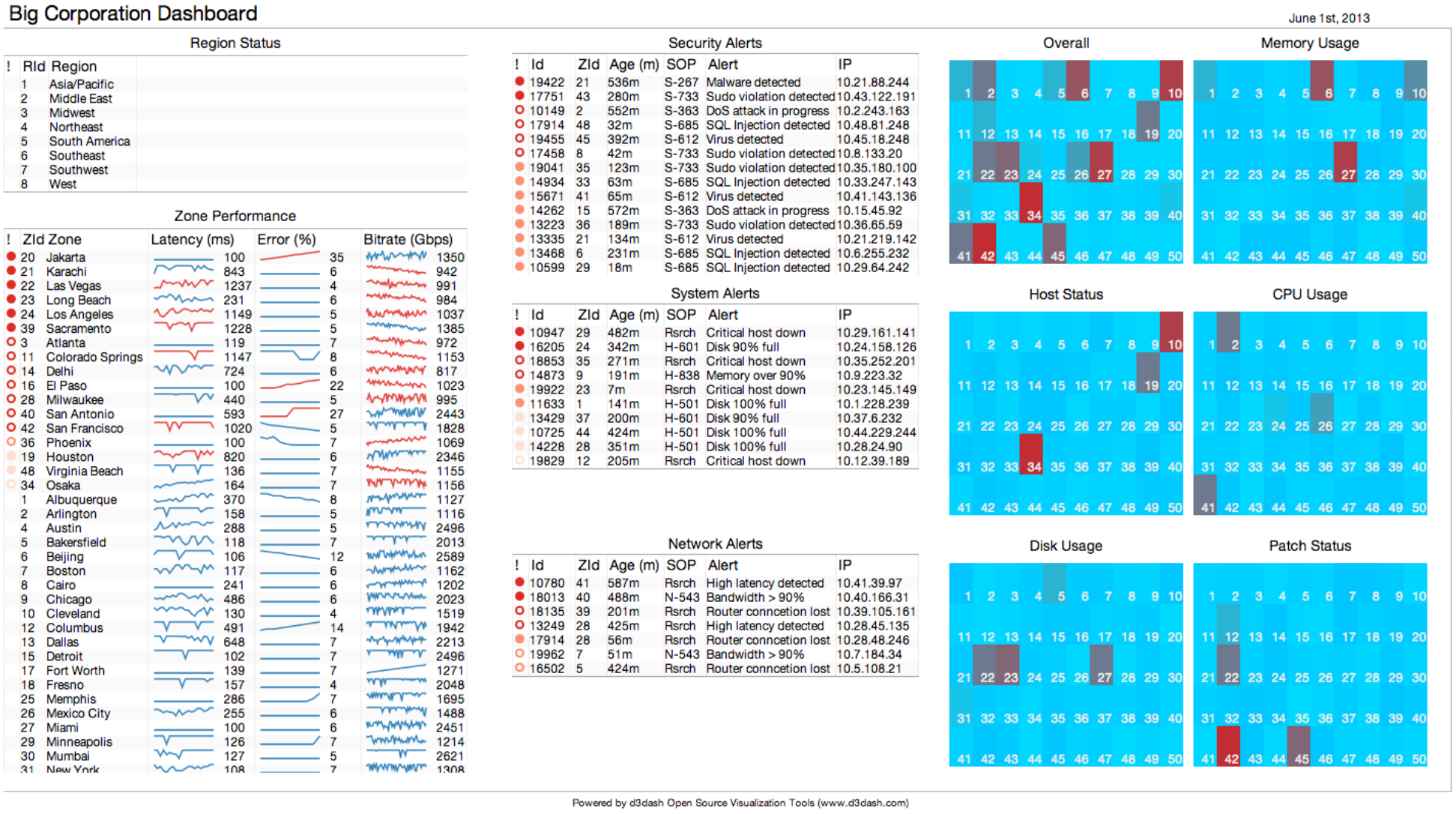
Notes

1. The team discussed having another way to visualize the performance/health data between all of the locations.
2. The 'yellow' is the headquarters location and the 'grey' cells represent a connection to the internet.
3. The team felt that this is a great way for displaying connections but may be hard to show multiple locations. One way to address this limitation would be to abbreviate the location names or leave out other data elements.

!	ZID	Subject	Type	Alert	Age	SOP
	6	10.39.28.39	System	10933 - Memory over 90 %	2hr	324
	30	22.48.28.08	Security	38887 - SQL Injection	30m	101
	12	74.92.44.22				
			Security	15887 - Virus Detected	12m	333
			Security	82922 - Malware Detected	11m	983
			Security	24242 - DLP Violation	10m	421
		corpuser@bigcorp.com	Security	47829 - Excessive sudo attempts	8m	422
		92.01.46.92	Network	15887 - Bandwidth > 90%	4hr	590
	45	32.36.201.5	System	28792 - Unknown App Problem	4m	Research

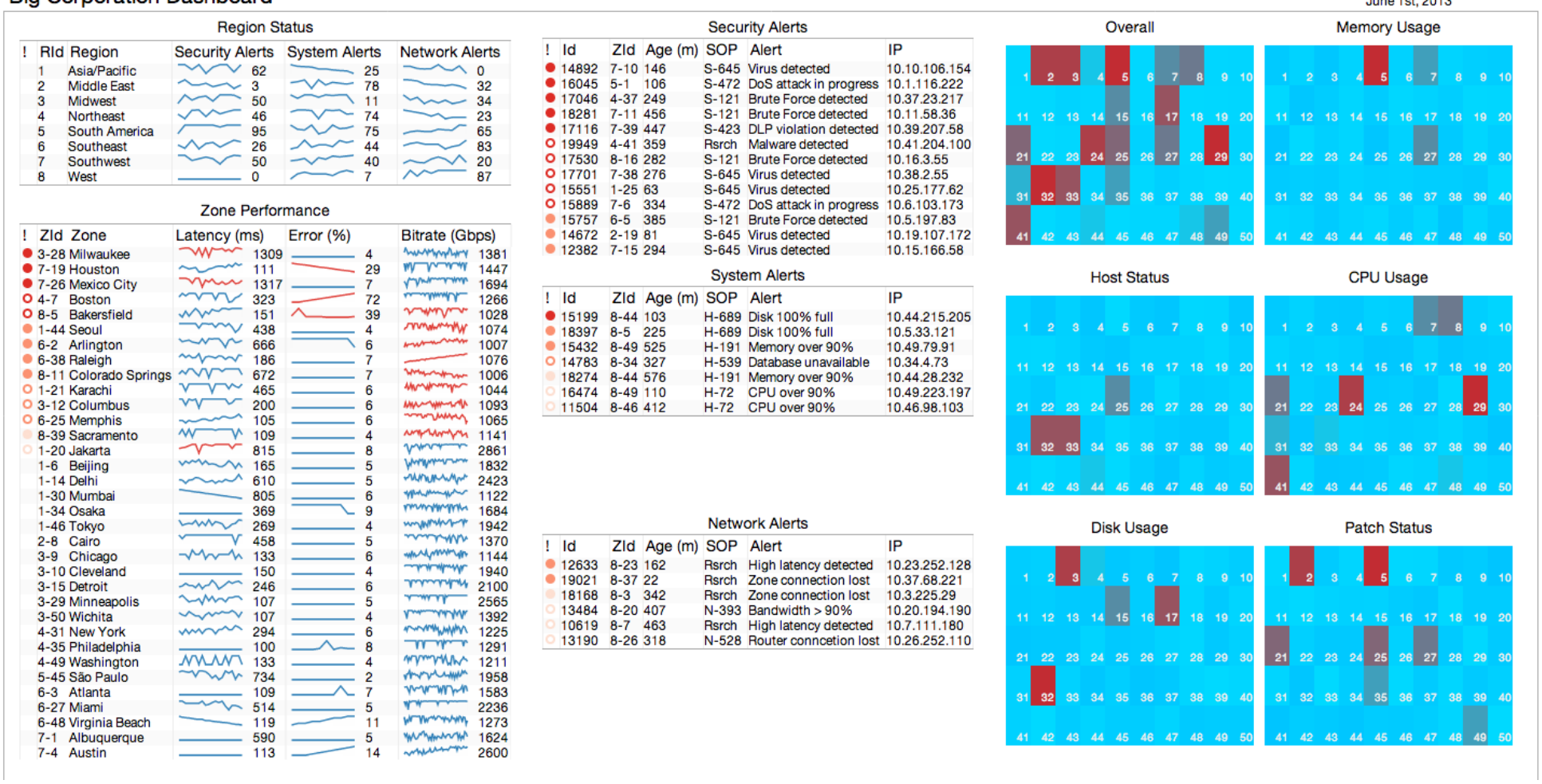
Notes

1. Another idea that surfaced from our discussions centered around the way to showing connections.
2. The goal for this grouping of alerts is to identify the Alert, Zone ID (ZID), and then by Subject.
3. The motivation for this was to isolate the region to view a series of events that may be related.
4. This design is pretty effective at showing connections, but this would be competing for the existing table format.



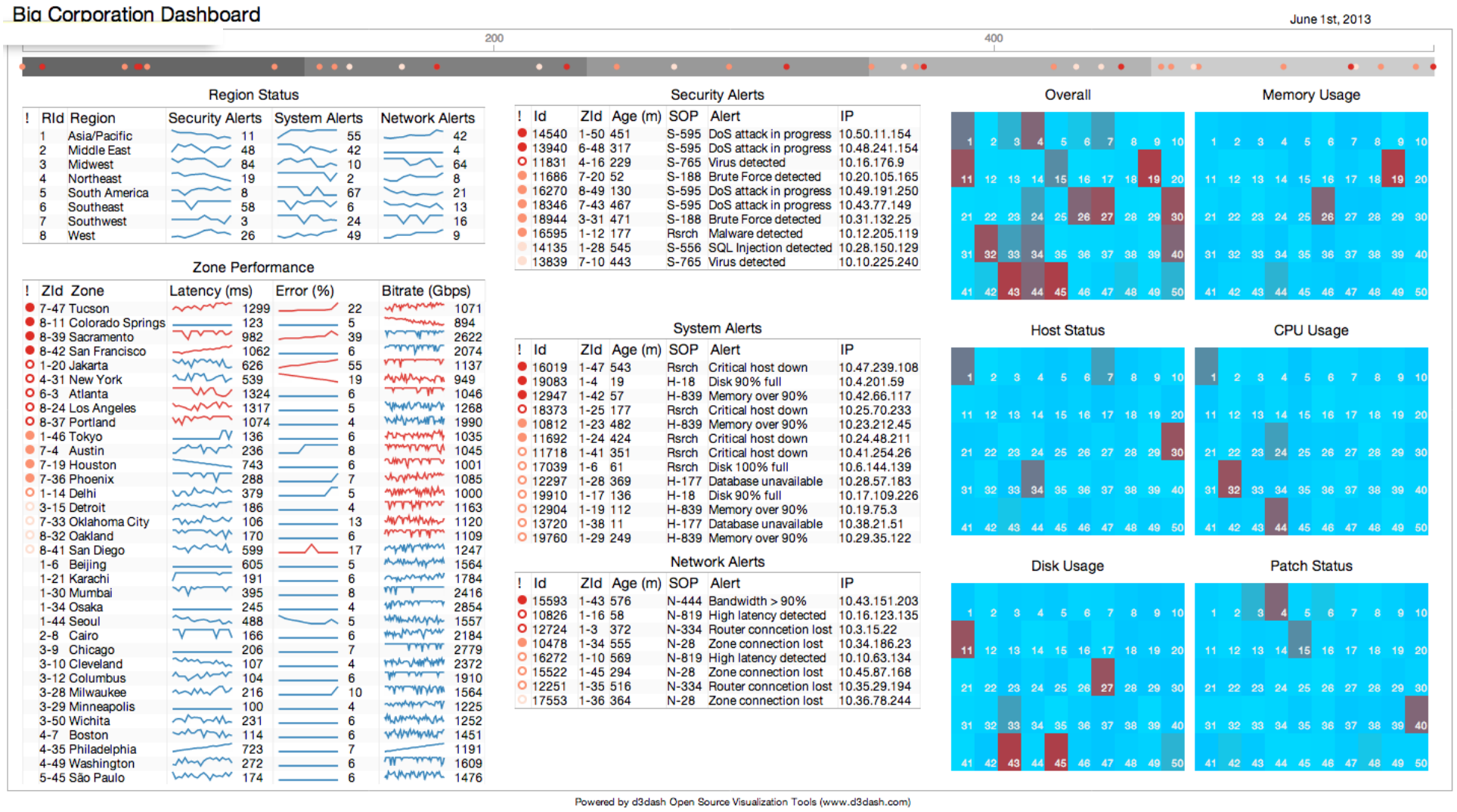
Notes

1. Zones can easily be increased/decreased with this design.
2. The Big Corporation has tools in place that can be used to monitor all the information provided on the dashboard.
3. Dashboard display (on large screen) will primarily be used for monitoring--the interactivity on the large screen will be purposefully very limited.
4. The team assumes that any analyst using the tools to create a dashboard will use their standard tools (SIEM or other) in order to further research, ticket, assign, and address the problems identified.
5. Alerts are given 3 levels of priority.
6. The "ZId" (Zone ID) is critical because it helps determine which team needs to be contacted when an event surfaces.
7. A 'Region Status' was added to the top of the dashboard.



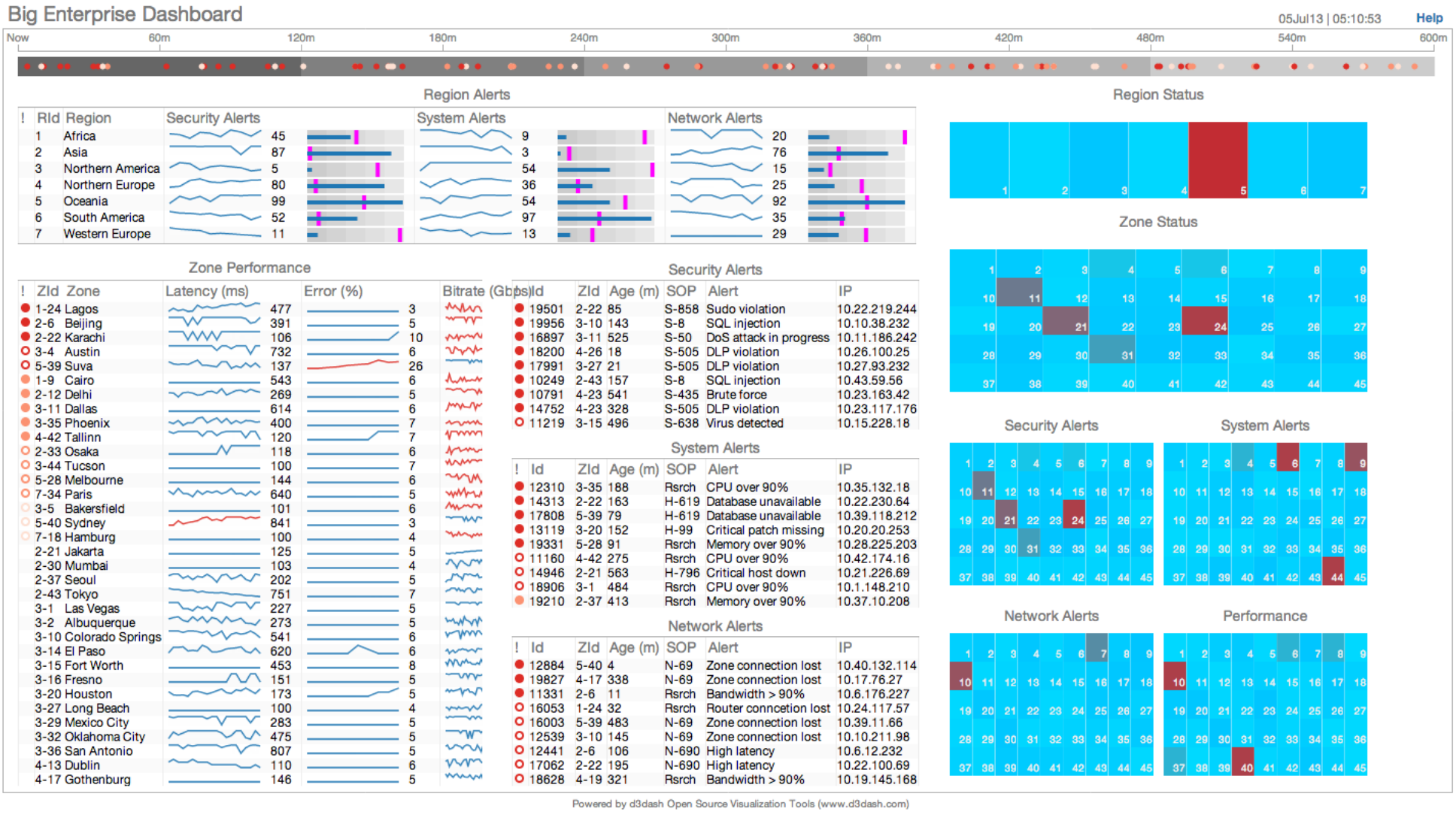
Notes

1. Region status was enhanced to include 'Sparklines', Security, System, and Network Alerts.



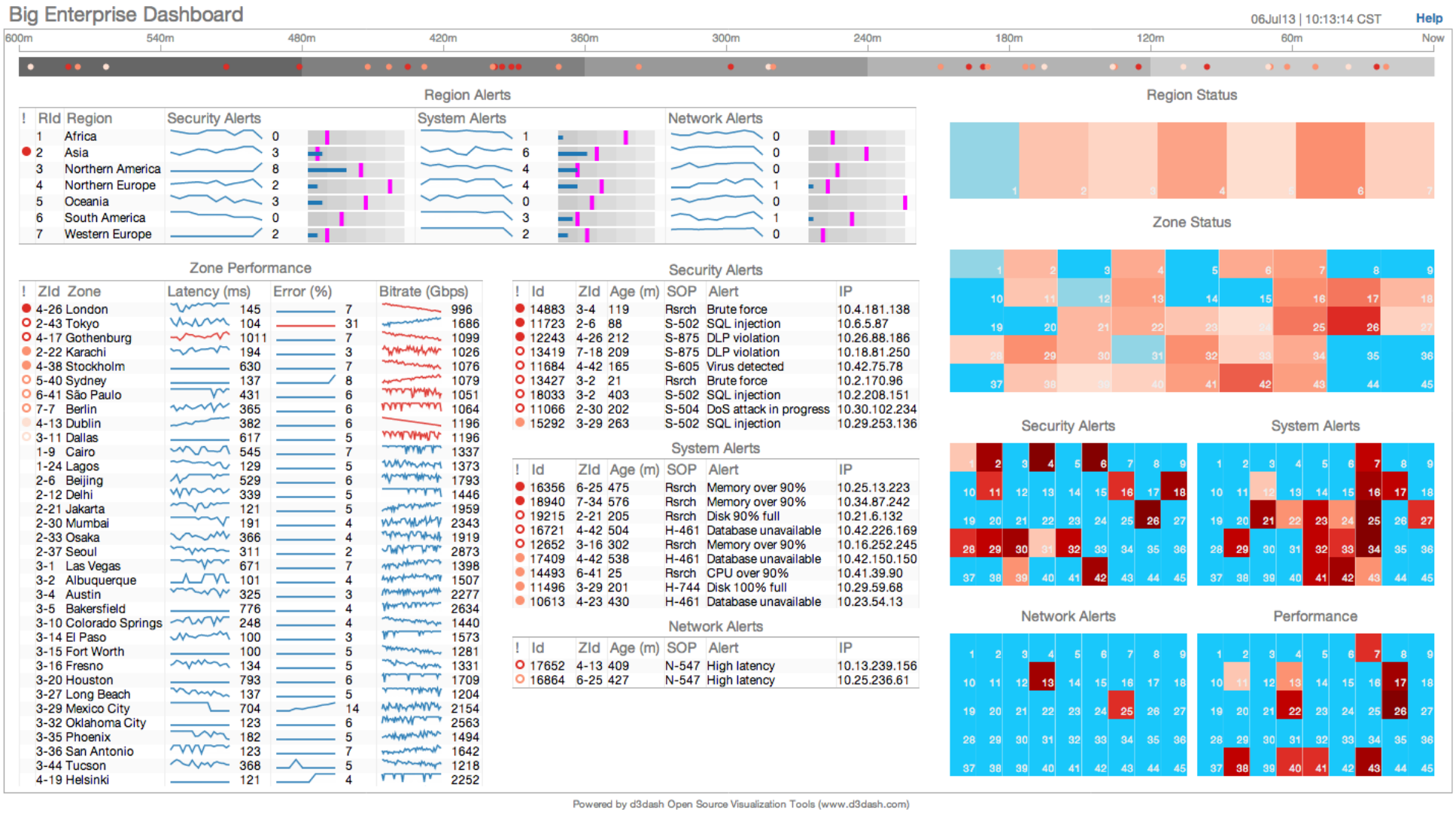
Notes

1. A timeline across the top of the dashboard was added.



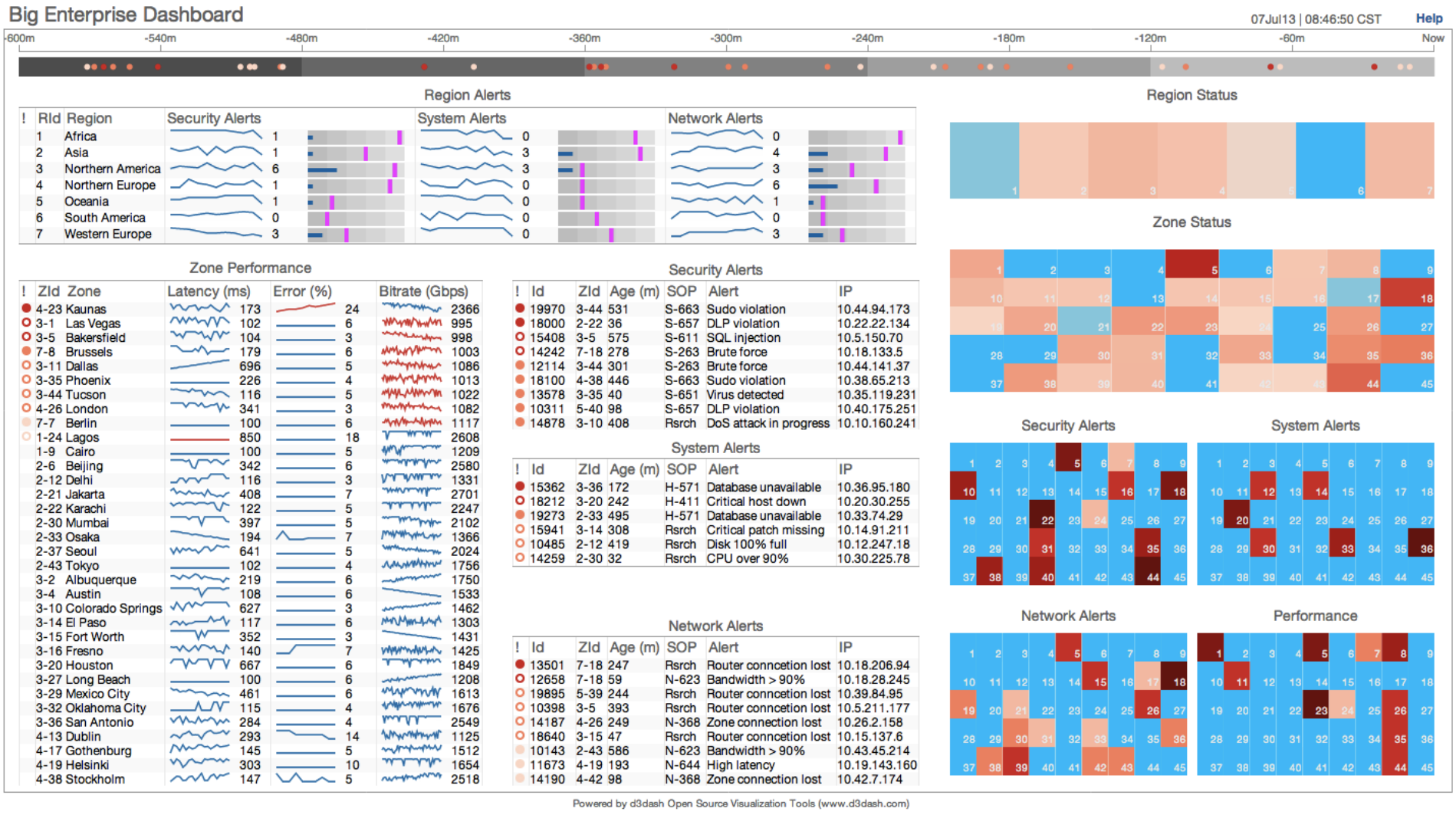
Notes

1. The name of the dashboard was changed from 'Big Corporate Dashboard' to 'Big Enterprise Dashboard'.
2. The Regions were modified by adopting the United Nations (UN) classification system for Regions and Sub-Regions.
3. A 'Help Button' was added to the upper right-hand side of the dashboard.
4. A time stamp was added using a military time format in the upper right-hand side of the dashboard.
5. Bullet graphs were added under the 'Region Alerts' for a quick display of activity.
6. The 'Alert Timeline' was confusing since it started with the 'Now' descriptor on the left – a future version will address this challenge.



Notes

1. A time stamp was added using a military time format in the upper right-hand side of the dashboard with the time zone after it.
2. The 'Alert Timeline' was flipped with the historical time stamp starting on the far left and the most current time on the far right.
3. The heatmaps are color coded based on a linear scale with light blue being good moving towards a red, which indicates that immediate attention is required.



Notes

1. The final dashboard has a minor modification – the timeline now has a negative (-) sign in front of the minutes to demonstrate that they occurred in the past.
2. This final version also has the ability to limit the number of regions experiencing critical issues.