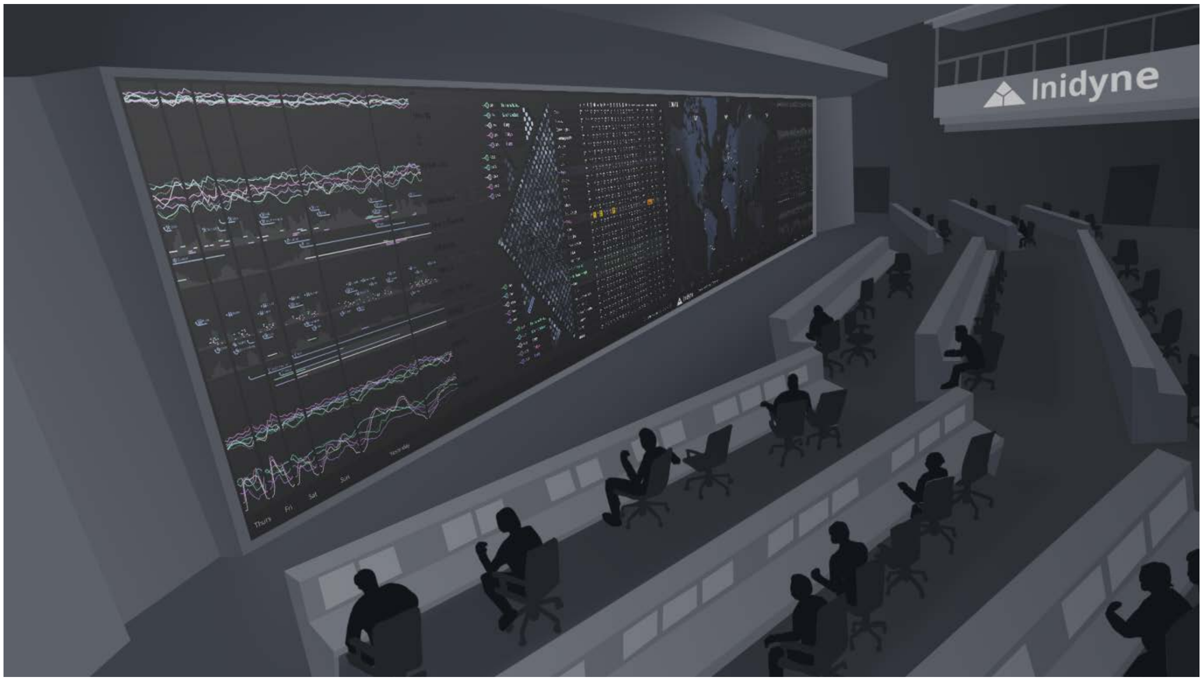
NOCturne - Storyboard

Entry for VAST 2013, Mini-Challenge 2: Situation Awareness Display Design



Riley Benson, Rajiv Ramarajan

7/8/13

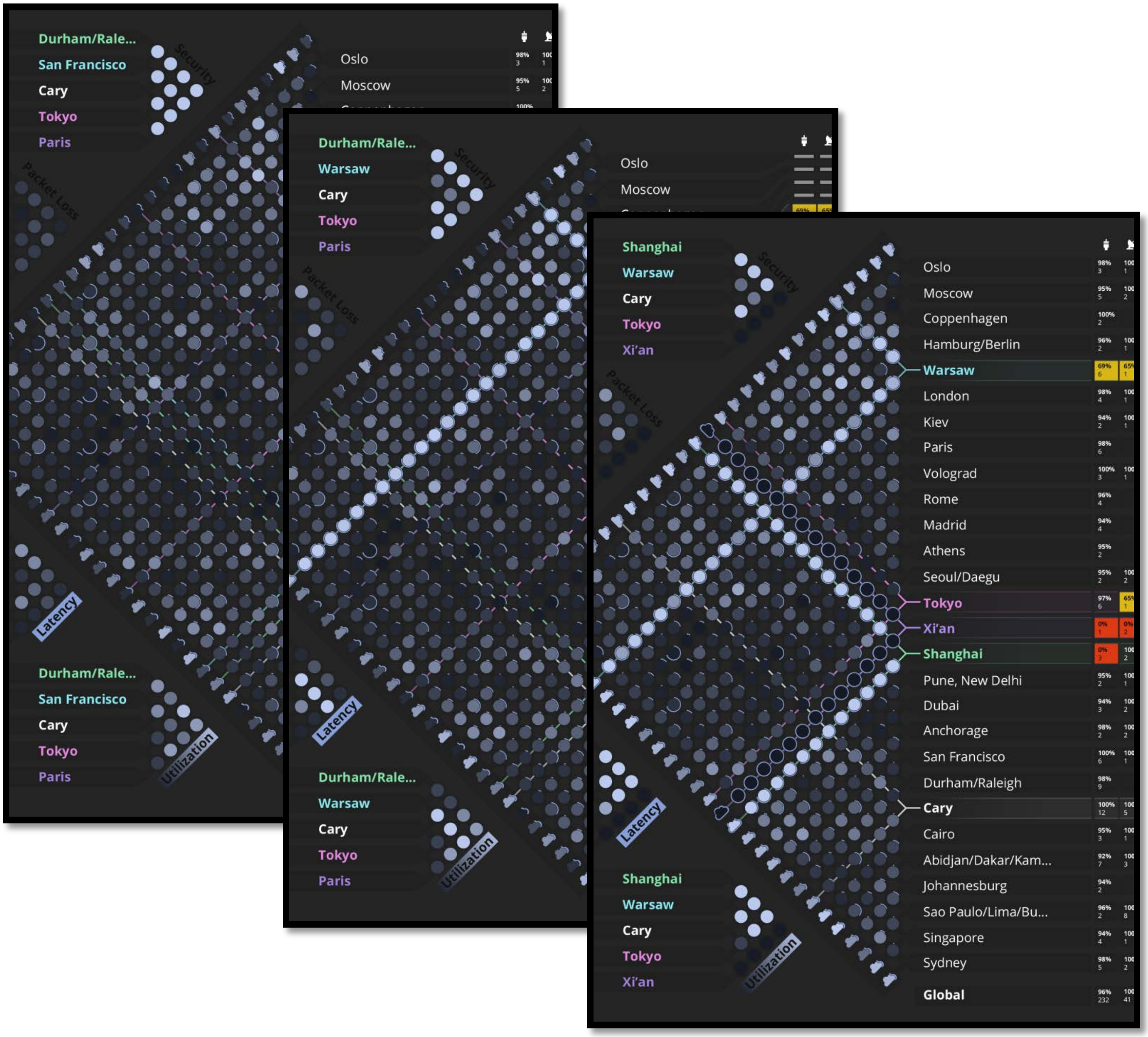
NOCturne setup

The NOCturne network operations monitor adjusts to particular business priorities and context in the following ways:

Location priorities

The NOCturne UI provides detailed metrics for locations that are most critical to the operation of the business, and recognizes that this may change based on the situation. As underlying context for selecting which locations to focus on a list of location priorities must be provided

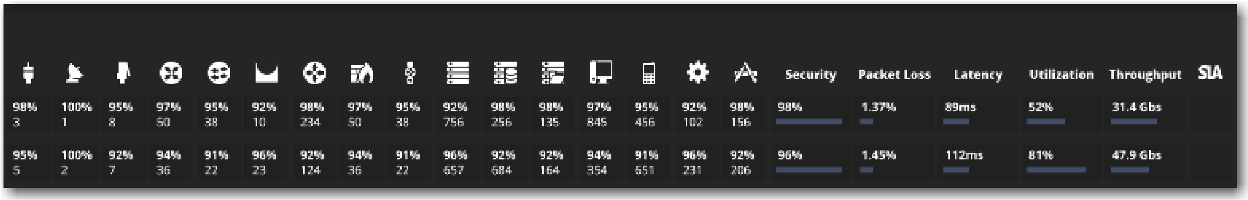
In the first image, we see the top 5 cities that are important for the company during normal operations. However, Warsaw replaces San Francisco as soon as abnormal activity is detected there. Finally, Shanghai and Xian are added as soon as an earthquake event sends those offices in a critical state. Note that Cary, the world headquarters of BIG Enterprise, is always shown due to its critical business impact.



Tracked metrics

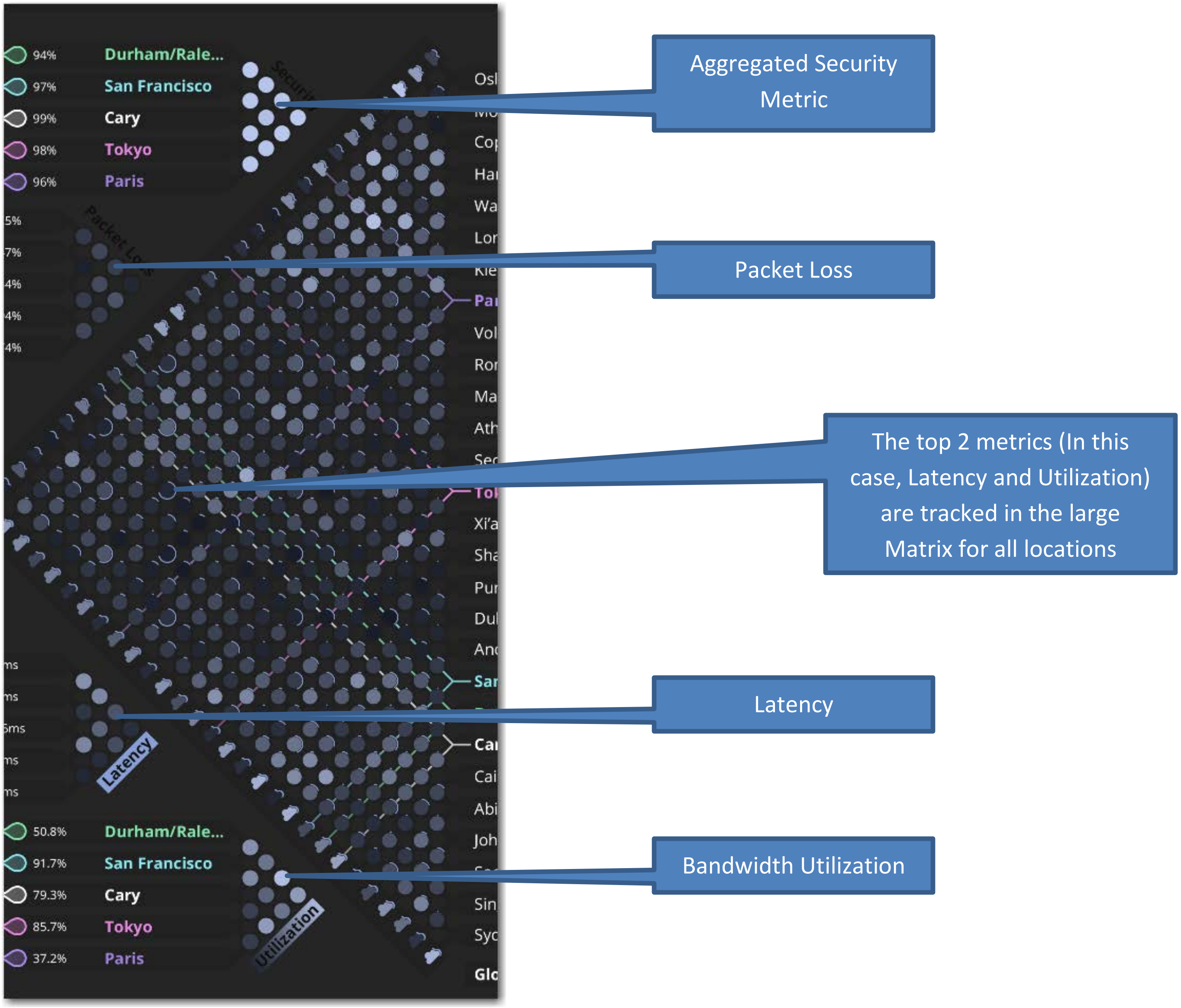
NOCturne presents the business metrics ordered based on the priority that they are given. This way more detail and visibility is provided for more critical metrics.

In the **Grid**, important business metrics are given columns after the columns for important network hardware and service health represented by icons:



																Security	Packet Loss	Latency	Utilization	Throughput	SLA
98% 3	100% 1	95% 8	97% 50	95% 38	92% 10	98% 234	97% 50	95% 38	92% 756	98% 256	98% 135	97% 845	95% 456	92% 102	98% 156	98%	1.37%	89ms	52%	31.4 Gbs	
95% 5	100% 2	92% 7	94% 36	91% 22	96% 23	92% 124	94% 36	91% 22	96% 657	92% 684	92% 164	94% 354	91% 651	96% 231	92% 206	96%	1.45%	112ms	81%	47.9 Gbs	

The top 4 measures for the business are tracked in the smaller **Matrices**. In the current scenario, they are Security, Packet Loss, Latency, and Bandwidth Utilization:



Aggregated Security Metric

Packet Loss

The top 2 metrics (In this case, Latency and Utilization) are tracked in the large Matrix for all locations

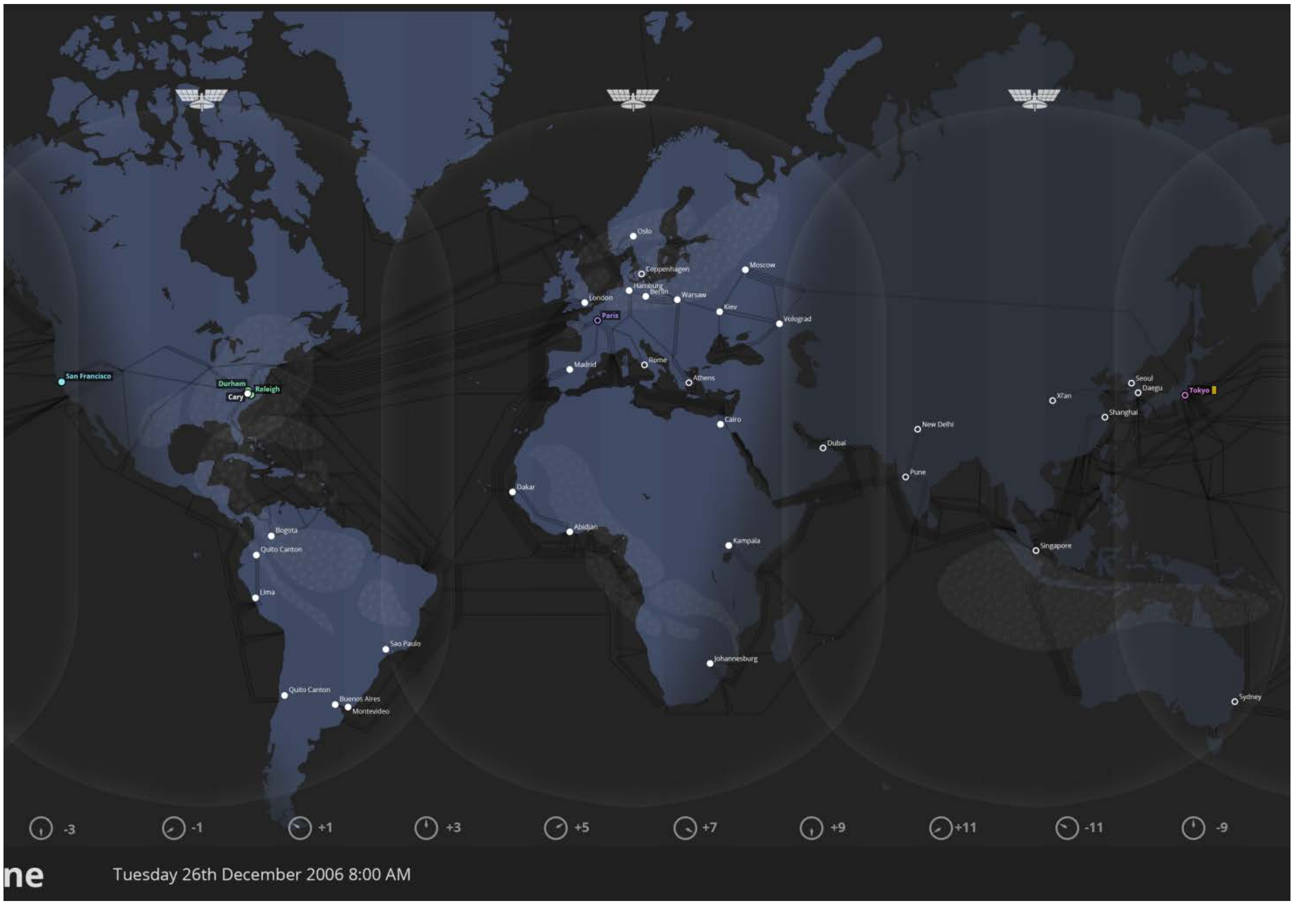
Latency

Bandwidth Utilization

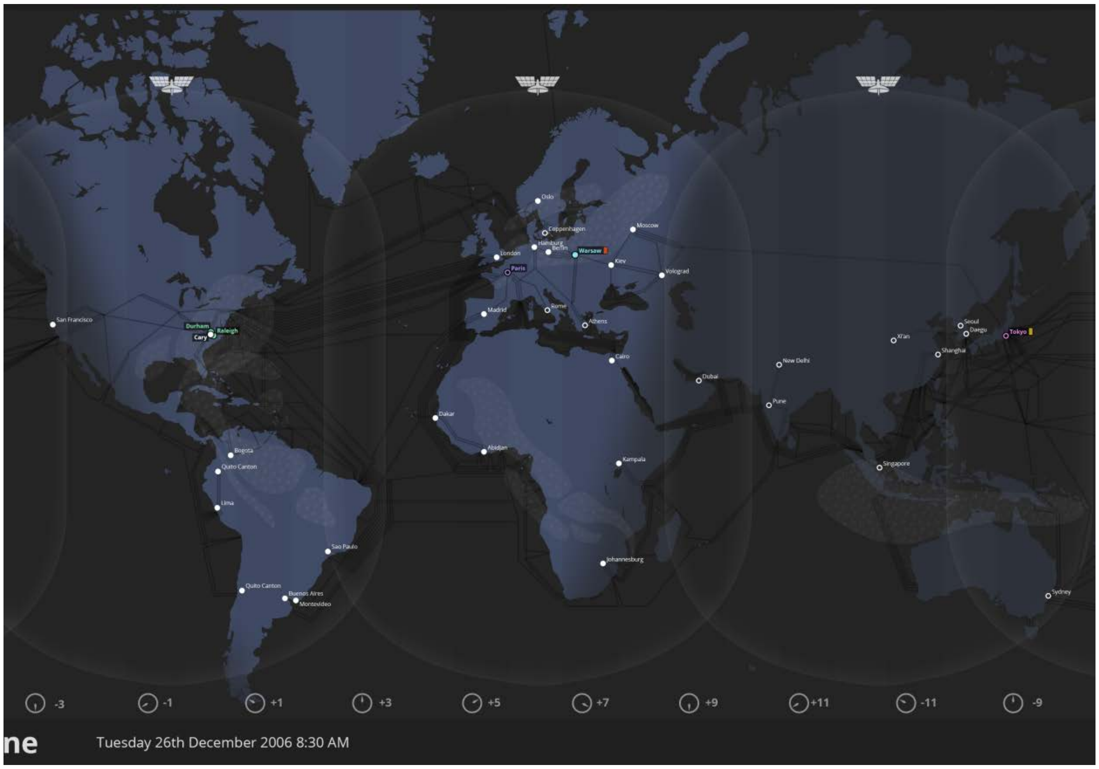
Information overlays on the Geomap

Overlays on the Geomap can be selected to reflect the factors that most affect business operation. This view shows:

1. Locations
    a. Global position of each location.
    b. Status of locations that have reached alert level.
    c. Whether an office is within business hours or not.
2. Connectivity and status of the land and undersea cables important for the business.
3. Day/night for the globe.
4. Current satellite coverage important for the business.
5. Weather patterns of significance.
6. Critical events such as an earthquake.

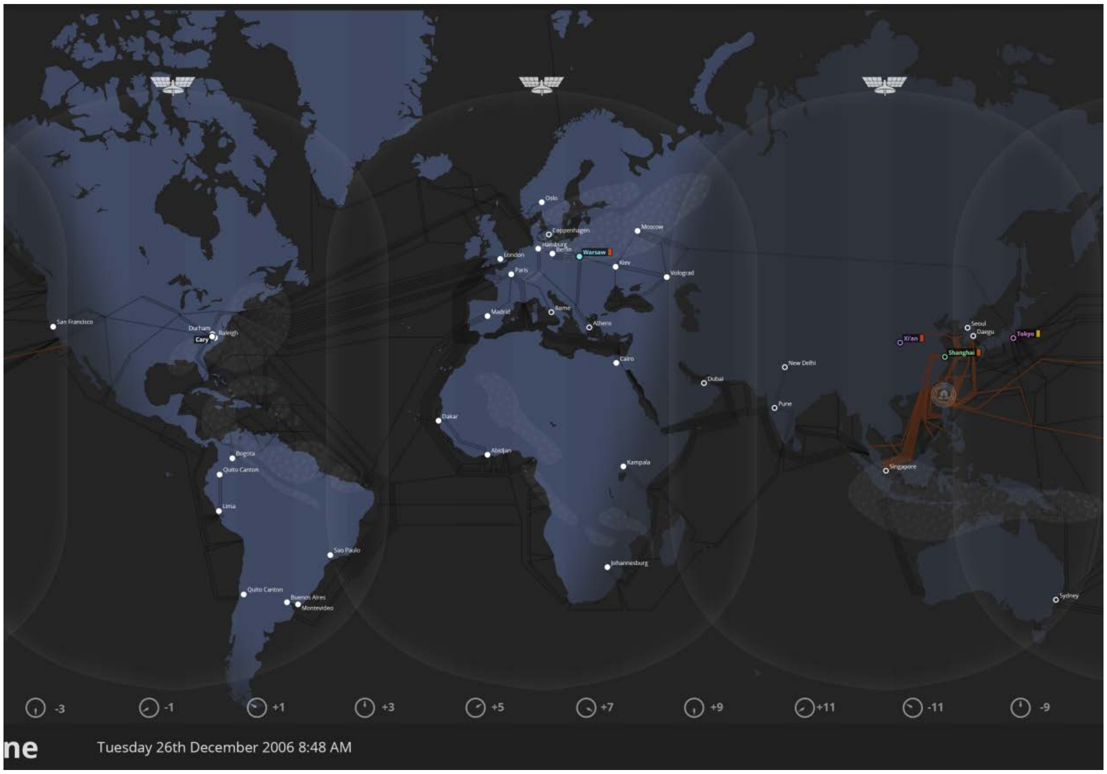


In this view the Warsaw office is highlighted as soon as the security metrics show abnormal readings:



Tuesday 26th December 2006 8:30 AM

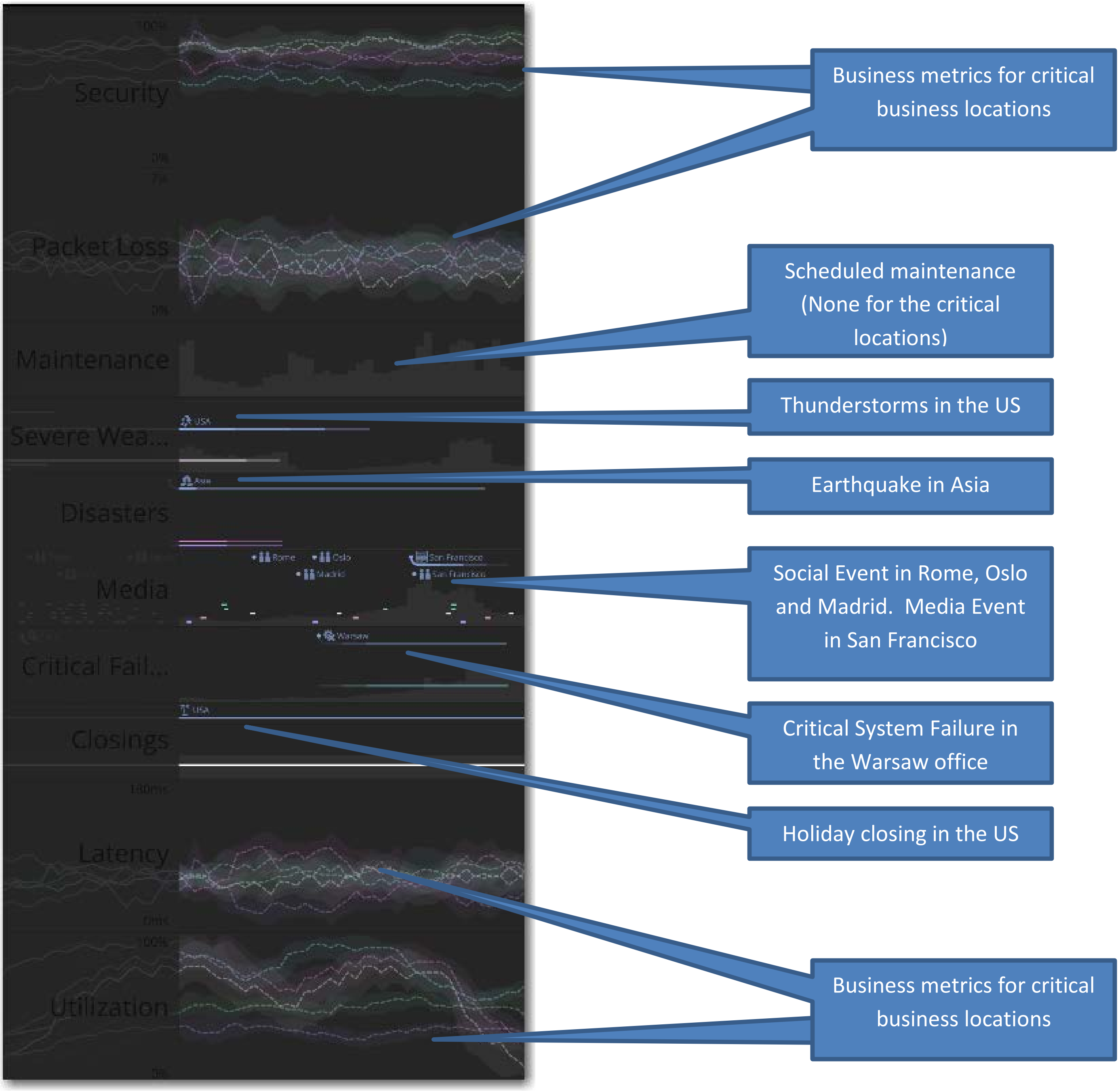
When the earthquake hits Taiwan, undersea and land cables are disrupted, and the Shanghai and Xian offices are highlighted as their performance and health metrics degrade:



Tuesday 26th December 2006 8:48 AM

Timeline

The **Timeline**, history and future, provides the NOC team with a consolidated view of all metrics, events, and business factors at a point in time. The combining of information into one UI from disparate sources, allows the team to quickly grasp the situation and make decisions.



Business metrics for critical business locations

Scheduled maintenance (None for the critical locations)

Thunderstorms in the US

Earthquake in Asia

Social Event in Rome, Oslo and Madrid. Media Event in San Francisco

Critical System Failure in the Warsaw office

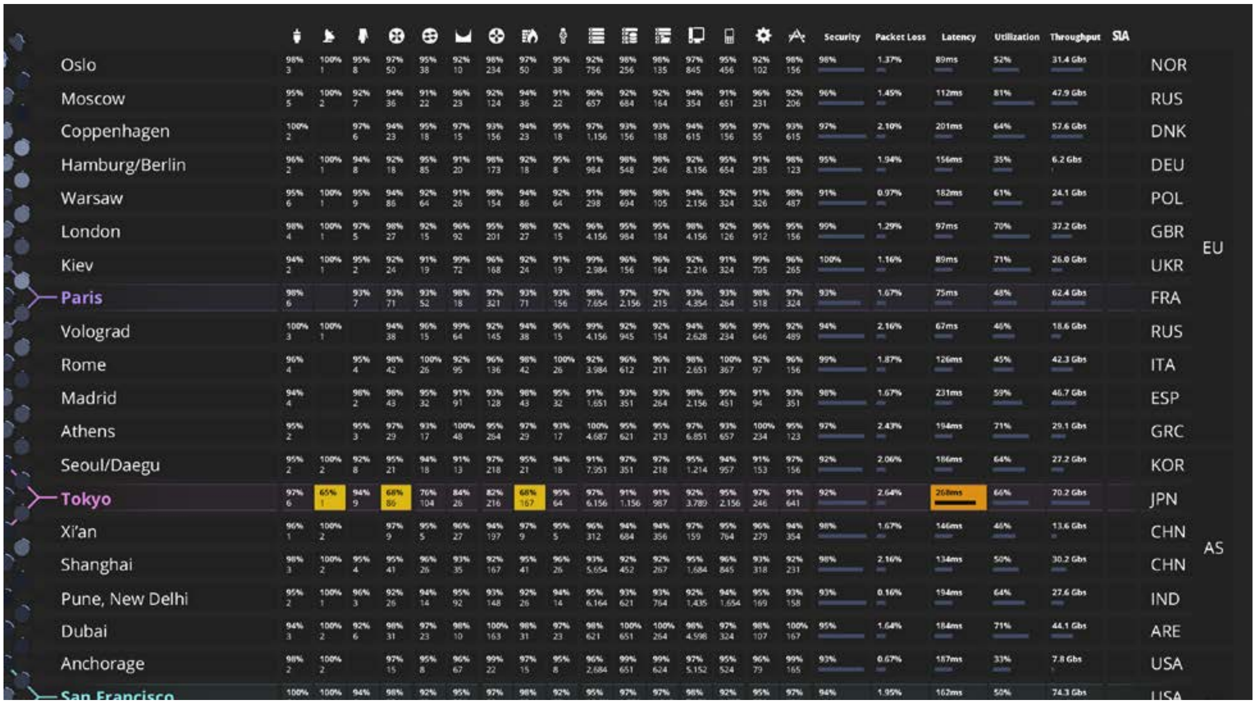
Holiday closing in the US

Business metrics for critical business locations

The UI samples the events displayed in detail based on the priority of the and highlighted for the locations that are in focus at that point of time.

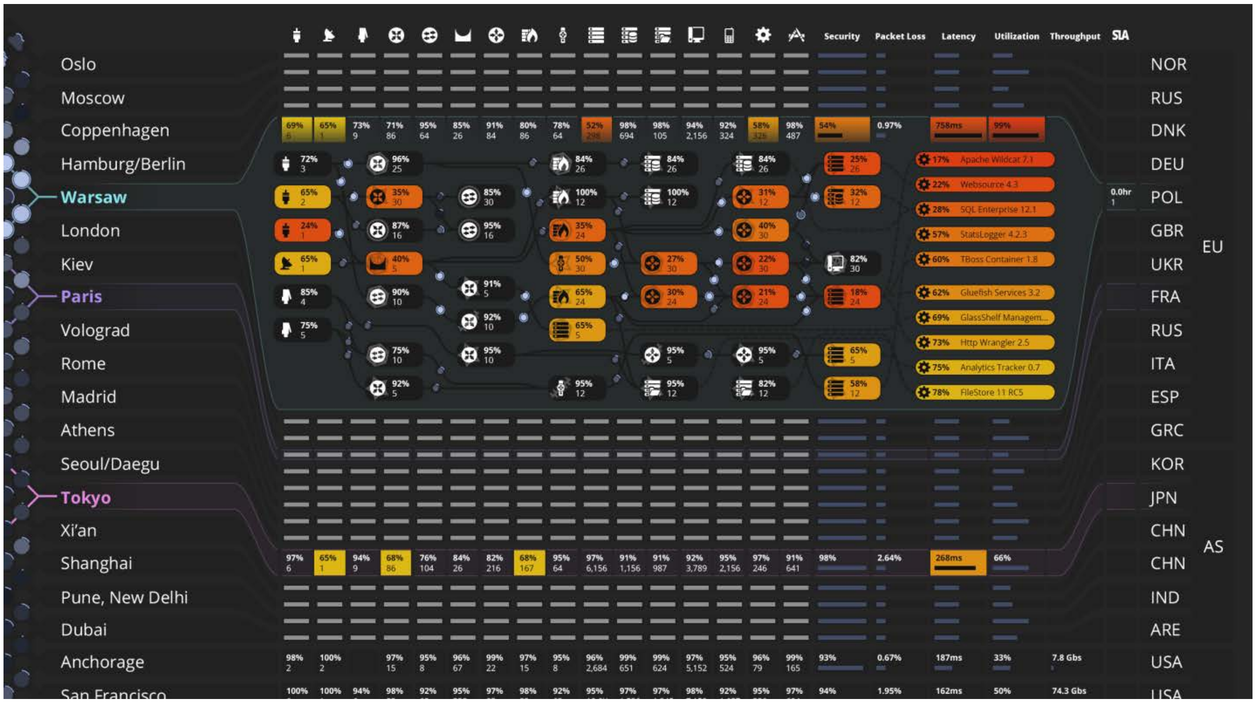
Displaying Detailed Topology

During normal operations, NOCturne displays performance, health and security metrics in rows for all locations.



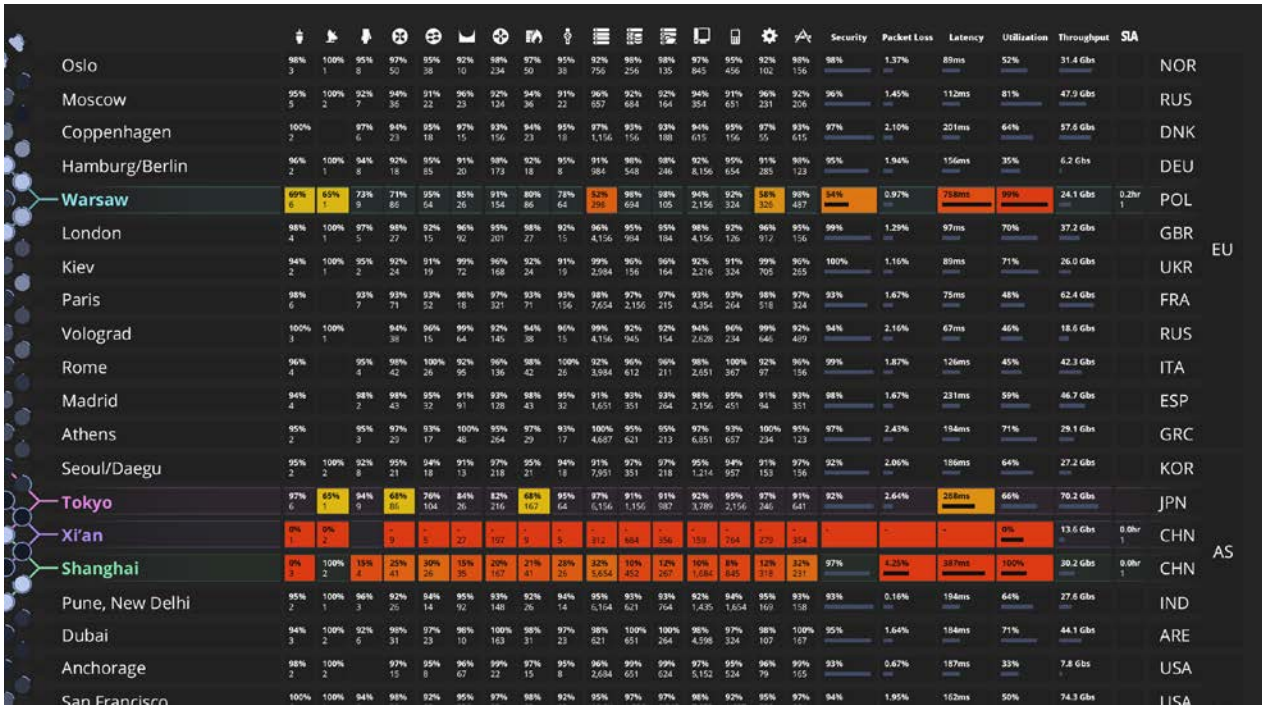
																	Security	Packet Loss	Latency	Utilization	Throughput	SIA		
Oslo	98% 3	100% 1	95% 8	97% 50	95% 38	92% 10	98% 234	97% 50	95% 38	92% 756	98% 256	98% 135	97% 845	95% 456	92% 102	98% 156	98%	1.37%	89ms	52%	31.4 Gbs		NOR	EU
Moscow	95% 5	100% 2	92% 7	94% 36	91% 22	96% 23	92% 124	94% 36	91% 22	96% 657	92% 684	92% 164	94% 354	91% 651	96% 231	92% 206	96%	1.45%	112ms	81%	47.9 Gbs		RUS	
Coppenhagen	100% 2		97% 6	94% 23	95% 18	97% 15	93% 156	94% 23	95% 18	97% 1,156	93% 156	93% 188	94% 615	95% 156	97% 55	93% 615	97%	2.10%	201ms	64%	57.6 Gbs		DNK	
Hamburg/Berlin	96% 2	100% 1	94% 8	92% 18	95% 85	91% 20	98% 173	92% 18	95% 8	91% 984	98% 548	98% 246	92% 8,156	95% 654	91% 285	98% 123	95%	1.94%	156ms	35%	6.2 Gbs		DEU	
Warsaw	95% 6	100% 1	95% 9	94% 86	92% 64	91% 26	98% 154	94% 86	92% 64	91% 298	98% 694	98% 105	94% 2,156	92% 324	91% 326	98% 487	91%	0.97%	182ms	61%	24.1 Gbs		POL	
London	98% 4	100% 1	97% 5	98% 27	92% 15	96% 92	95% 201	98% 27	92% 15	96% 4,156	95% 984	95% 184	98% 4,156	92% 126	96% 912	95% 156	99%	1.29%	97ms	70%	37.2 Gbs		GBR	
Kiev	94% 2	100% 1	95% 2	92% 24	91% 19	99% 72	96% 168	92% 24	91% 19	99% 2,984	96% 156	96% 164	92% 2,216	91% 324	99% 705	96% 265	100%	1.16%	89ms	71%	26.0 Gbs		UKR	
Paris	98% 6		93% 7	93% 71	93% 52	98% 18	97% 321	93% 71	93% 156	98% 7,654	97% 2,156	97% 215	93% 4,354	93% 264	98% 518	97% 324	93%	1.67%	75ms	48%	62.4 Gbs		FRA	
Volograd	100% 3	100% 1		94% 38	96% 15	99% 64	92% 145	94% 38	96% 15	99% 4,156	92% 945	92% 154	94% 2,628	96% 234	99% 646	92% 489	94%	2.16%	67ms	46%	18.6 Gbs		RUS	
Rome	96% 4		95% 4	98% 42	100% 26	92% 95	96% 136	98% 42	100% 26	92% 3,984	96% 612	96% 211	98% 2,651	100% 367	92% 97	96% 156	99%	1.87%	126ms	45%	42.3 Gbs		ITA	
Madrid	94% 4		98% 2	98% 43	95% 32	91% 91	93% 128	98% 43	95% 32	91% 1,651	93% 351	93% 264	98% 2,156	95% 451	91% 94	93% 351	98%	1.67%	231ms	59%	46.7 Gbs		ESP	
Athens	95% 2		95% 3	97% 29	93% 17	100% 48	95% 264	97% 29	93% 17	100% 4,687	95% 621	95% 213	97% 6,851	93% 657	100% 234	95% 123	97%	2.43%	194ms	71%	29.1 Gbs		GRC	
Seoul/Daegu	95% 2	100% 2	92% 8	95% 21	94% 18	91% 13	97% 218	95% 21	94% 18	91% 7,951	97% 351	97% 218	95% 1,214	94% 957	91% 153	97% 156	92%	2.06%	186ms	64%	27.2 Gbs		KOR	AS
Tokyo	97% 6	65% 1	94% 9	68% 86	76% 104	84% 26	82% 216	68% 167	95% 64	97% 6,156	91% 1,156	91% 987	92% 3,789	95% 2,156	97% 246	91% 641	92%	2.64%	268ms	66%	70.2 Gbs		JPN	
Xi'an	96% 1	100% 2		97% 9	95% 5	96% 27	94% 197	97% 9	95% 5	96% 312	94% 684	94% 356	97% 159	95% 764	96% 279	94% 354	98%	1.67%	146ms	46%	13.6 Gbs		CHN	
Shanghai	98% 3	100% 2	95% 4	95% 41	96% 26	93% 35	92% 167	95% 41	96% 26	93% 5,654	92% 452	92% 267	95% 1,684	96% 845	93% 318	92% 231	98%	2.16%	134ms	50%	30.2 Gbs		CHN	
Pune, New Delhi	95% 2	100% 1	96% 3	92% 26	94% 14	95% 92	93% 148	92% 26	94% 14	95% 6,164	93% 621	93% 764	92% 1,435	94% 1,654	95% 169	93% 158	93%	0.16%	194ms	64%	27.6 Gbs		IND	
Dubai	94% 3	100% 2	92% 6	98% 31	97% 23	98% 10	100% 163	98% 31	97% 23	98% 621	100% 651	100% 264	98% 4,598	97% 324	98% 107	100% 167	95%	1.64%	184ms	71%	44.1 Gbs		ARE	
Anchorage	98% 2	100% 2		97% 15	95% 8	96% 67	99% 22	97% 15	95% 8	96% 2,684	99% 651	99% 624	97% 5,152	95% 524	96% 79	99% 165	93%	0.67%	187ms	33%	7.8 Gbs		USA	
San Francisco	100%	100%	94%	98%	92%	95%	97%	98%	92%	95%	97%	97%	98%	92%	95%	97%	94%	1.95%	162ms	50%	74.3 Gbs		USA	

As soon as NOCturne detects substantially abnormal system metrics for a certain location, and it is the only location experiencing severe issues, a detailed topology is automatically opened for that location. In this view Warsaw has a detailed topology displayed. As a result of this expansion some information for non-critical systems is compressed but still displayed to allow for continued monitoring:



																	Security	Packet Loss	Latency	Utilization	Throughput	SIA		
Oslo																							NOR	EU
Moscow																							RUS	
Coppenhagen	69% 6	65% 1	73% 9	71% 86	95% 64	85% 26	91% 84	80% 86	78% 64	52% 298	98% 694	98% 105	94% 2,156	92% 324	58% 326	98% 487	54%	0.97%	758ms	99%			DNK	
Hamburg/Berlin																							DEU	
Warsaw																						0.0hr 1	POL	
London																							GBR	
Kiev																							UKR	
Paris																							FRA	
Volograd																							RUS	
Rome																							ITA	
Madrid																							ESP	
Athens																							GRC	
Seoul/Daegu																							KOR	AS
Tokyo																							JPN	
Xi'an																							CHN	
Shanghai	97% 6	65% 1	94% 9	68% 86	76% 104	84% 26	82% 216	68% 167	95% 64	97% 6,156	91% 1,156	91% 987	92% 3,789	95% 2,156	97% 246	91% 641	98%	2.64%	268ms	66%			CHN	
Pune, New Delhi																							IND	
Dubai																							ARE	
Anchorage	98% 2	100% 2		97% 15	95% 8	96% 67	99% 22	97% 15	95% 8	96% 2,684	99% 651	99% 624	97% 5,152	95% 524	96% 79	99% 165	93%	0.67%	187ms	33%	7.8 Gbs		USA	
San Francisco	100%	100%	94%	98%	92%	95%	97%	98%	92%	95%	97%	97%	98%	92%	95%	97%	94%	1.95%	162ms	50%	74.3 Gbs		USA	

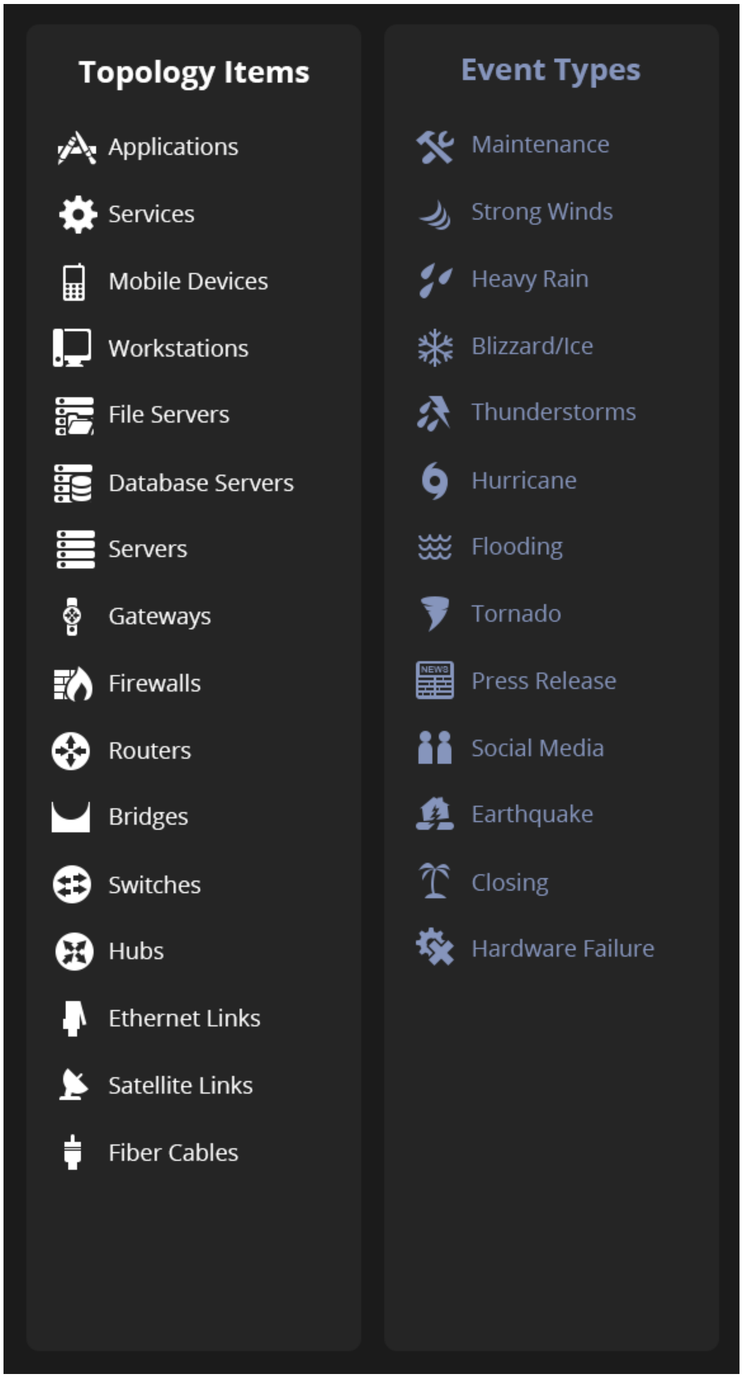
In the case when multiple system failures are detected, (The denial of service in Warsaw, and Earthquake effects in Shanghai and Xian) the detail topology closes to show the grid rows with summarized metrics but this time with indicators highlighting the critical states.



																	Security	Packet Loss	Latency	Utilization	Throughput	SLA		
Oslo	98% 3	100% 1	95% 8	97% 50	95% 38	92% 10	98% 234	97% 50	95% 38	92% 756	98% 256	98% 135	97% 845	95% 456	92% 102	98% 156	98%	1.37%	89ms	52%	31.4 Gbs		NOR	EU
Moscow	95% 5	100% 2	92% 7	94% 36	91% 22	96% 23	92% 124	94% 36	91% 22	96% 657	92% 684	92% 164	94% 354	91% 651	96% 231	92% 206	96%	1.45%	112ms	81%	47.9 Gbs		RUS	
Coppenhagen	100% 2		97% 6	94% 23	95% 18	97% 15	93% 156	94% 23	95% 18	97% 1,156	93% 156	93% 188	94% 615	95% 156	97% 55	93% 615	97%	2.10%	201ms	64%	57.6 Gbs		DNK	
Hamburg/Berlin	96% 2	100% 1	94% 8	92% 18	95% 85	91% 20	98% 173	92% 18	95% 8	91% 984	98% 548	98% 246	92% 8,156	95% 654	91% 285	98% 123	95%	1.94%	156ms	35%	6.2 Gbs		DEU	
Warsaw	69% 6	65% 1	73% 9	71% 86	95% 64	85% 26	91% 154	80% 86	78% 64	52% 298	98% 694	98% 105	94% 2,156	92% 324	58% 326	98% 487	54%	0.97%	758ms	99%	24.1 Gbs	0.2hr 1	POL	
London	98% 4	100% 1	97% 5	98% 27	92% 15	96% 92	95% 201	98% 27	92% 15	96% 4,156	95% 984	95% 184	98% 4,156	92% 126	96% 912	95% 156	99%	1.29%	97ms	70%	37.2 Gbs		GBR	
Kiev	94% 2	100% 1	95% 2	92% 24	91% 19	99% 72	96% 168	92% 24	91% 19	99% 2,984	96% 156	96% 164	92% 2,216	91% 324	99% 705	96% 265	100%	1.16%	89ms	71%	26.0 Gbs		UKR	
Paris	98% 6		93% 7	93% 71	93% 52	98% 18	97% 321	93% 71	93% 156	98% 7,654	97% 2,156	97% 215	93% 4,354	93% 264	98% 518	97% 324	93%	1.67%	75ms	48%	62.4 Gbs		FRA	
Volograd	100% 3	100% 1		94% 38	96% 15	99% 64	92% 145	94% 38	96% 15	99% 4,156	92% 945	92% 154	94% 2,628	96% 234	99% 646	92% 489	94%	2.16%	67ms	46%	18.6 Gbs		RUS	
Rome	96% 4		95% 4	98% 42	100% 26	92% 95	96% 136	98% 42	100% 26	92% 3,984	96% 612	96% 211	98% 2,651	100% 367	92% 97	96% 156	99%	1.87%	126ms	45%	42.3 Gbs		ITA	
Madrid	94% 4		98% 2	98% 43	95% 32	91% 91	93% 128	98% 43	95% 32	91% 1,651	93% 351	93% 264	98% 2,156	95% 451	91% 94	93% 351	98%	1.67%	231ms	59%	46.7 Gbs		ESP	
Athens	95% 2		95% 3	97% 29	93% 17	100% 48	95% 264	97% 29	93% 17	100% 4,687	95% 621	95% 213	97% 6,851	93% 657	100% 234	95% 123	97%	2.43%	194ms	71%	29.1 Gbs		GRC	
Seoul/Daegu	95% 2	100% 2	92% 8	95% 21	94% 18	91% 13	97% 218	95% 21	94% 18	91% 7,951	97% 351	97% 218	95% 1,214	94% 957	91% 153	97% 156	92%	2.06%	186ms	64%	27.2 Gbs		KOR	AS
Tokyo	97% 6	65% 1	94% 9	68% 86	76% 104	84% 26	82% 216	68% 167	95% 64	97% 6,156	91% 1,156	91% 987	92% 3,789	95% 2,156	97% 246	91% 641	92%	2.64%	288ms	66%	70.2 Gbs		JPN	
Xi'an	0% 1	0% 2		- 9	- 5	- 27	- 197	- 9	- 5	- 312	- 684	- 356	- 159	- 764	- 279	- 354	-	-	-	0%	13.6 Gbs	0.0hr 1	CHN	
Shanghai	0% 3	100% 2	15% 4	25% 41	30% 26	15% 35	20% 167	21% 41	28% 26	32% 5,654	10% 452	12% 267	10% 1,684	8% 845	12% 318	32% 231	97%	4.25%	387ms	100%	30.2 Gbs	0.0hr 1	CHN	
Pune, New Delhi	95% 2	100% 1	96% 3	92% 26	94% 14	95% 92	93% 148	92% 26	94% 14	95% 6,164	93% 621	93% 764	92% 1,435	94% 1,654	95% 169	93% 158	93%	0.16%	194ms	64%	27.6 Gbs		IND	
Dubai	94% 3	100% 2	92% 6	98% 31	97% 23	98% 10	100% 163	98% 31	97% 23	98% 621	100% 651	100% 264	98% 4,598	97% 324	98% 107	100% 167	95%	1.64%	184ms	71%	44.1 Gbs		ARE	
Anchorage	98% 2	100% 2		97% 15	95% 8	96% 67	99% 22	97% 15	95% 8	96% 2,684	99% 651	99% 624	97% 5,152	95% 524	96% 79	99% 165	93%	0.67%	187ms	33%	7.8 Gbs		USA	
San Francisco	100%	100%	94%	98%	92%	95%	97%	98%	92%	95%	97%	97%	98%	92%	95%	97%	94%	1.95%	162ms	50%	74.3 Gbs		USA	

Legend

Legend information can be accessed from workstations via applications linked to NOCturne. The legend provides reference for the data mappings and meaning of the various icons used in the display:



Topology Items

- Applications
- Services
- Mobile Devices
- Workstations
- File Servers
- Database Servers
- Servers
- Gateways
- Firewalls
- Routers
- Bridges
- Switches
- Hubs
- Ethernet Links
- Satellite Links
- Fiber Cables

Event Types

- Maintenance
- Strong Winds
- Heavy Rain
- Blizzard/Ice
- Thunderstorms
- Hurricane
- Flooding
- Tornado
- Press Release
- Social Media
- Earthquake
- Closing
- Hardware Failure