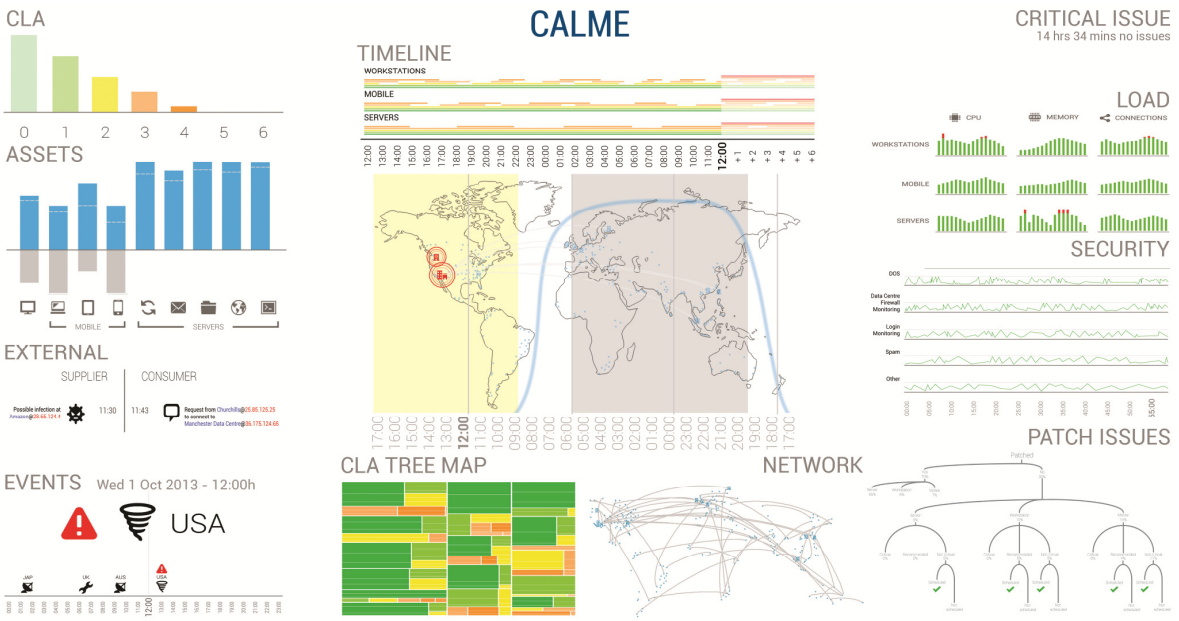
VAST 2013 - Mini Challenge 2

Cyber AnaLysis & Monitoring Environment (CALME)

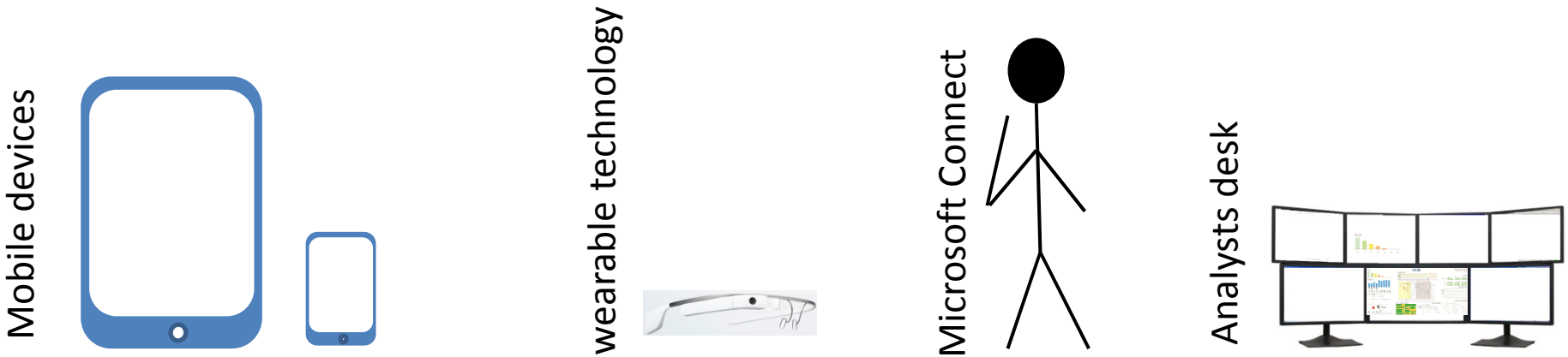
Tinni Choudhury, Neesha Kodagoda, Ashley Wheat, Puja Varsani, William Wong, Simon Attfield, Glenford Mapp, Louis Slabbert, Mahdi Aiash, Chris Rooney

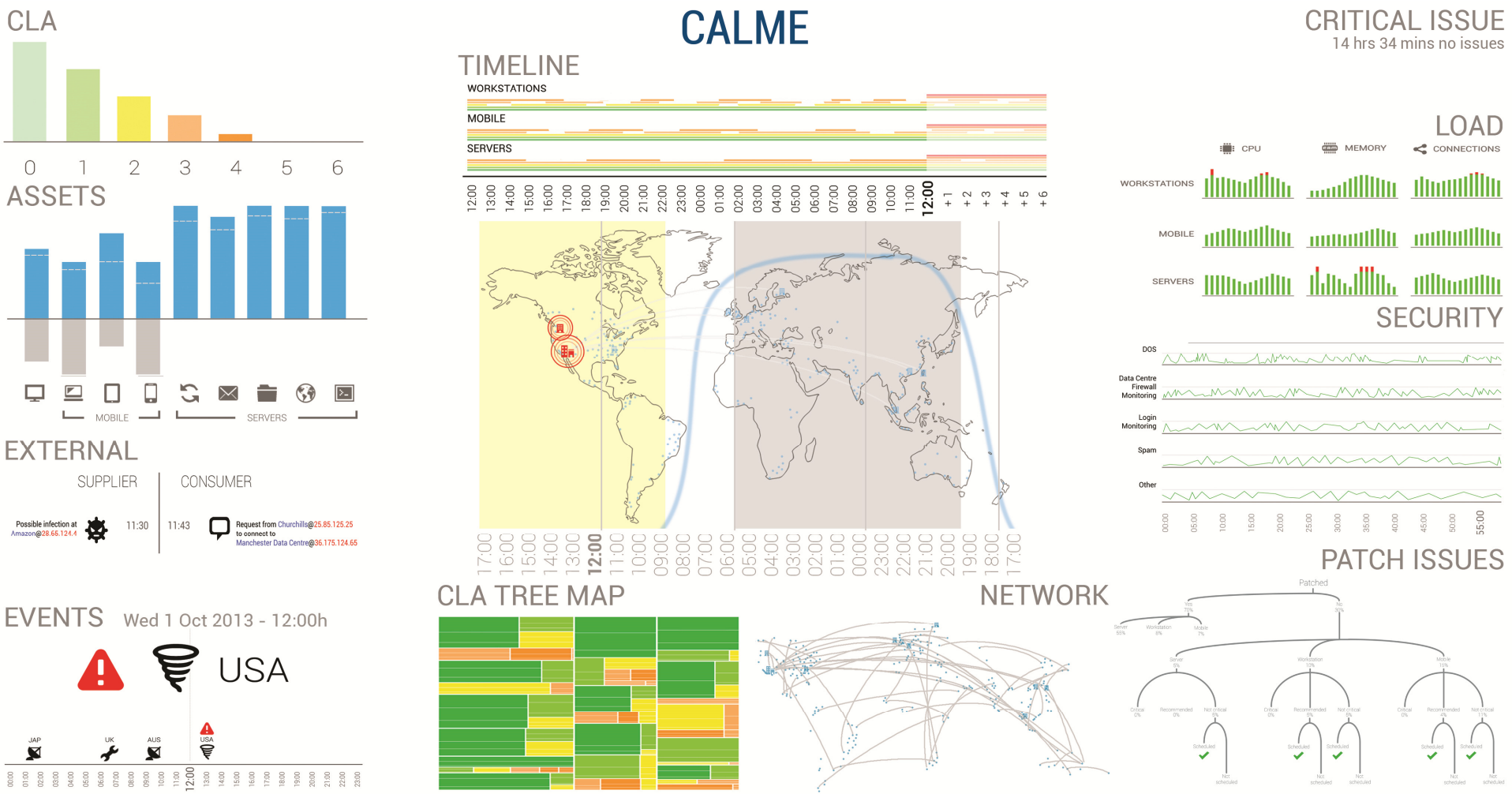
School of Science and Technology
Middlesex University, London
United Kingdom

Situation awareness operation centre

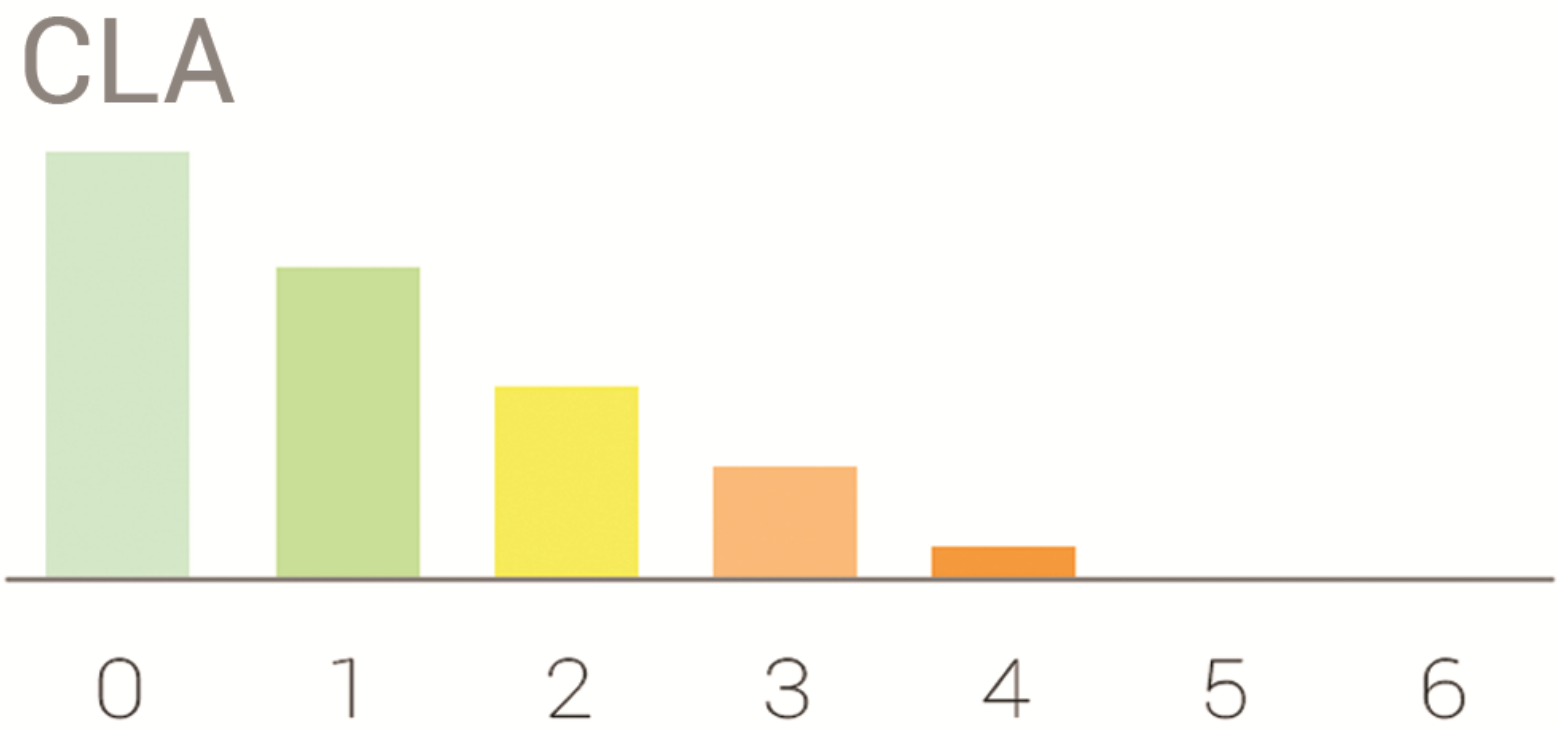


Drill down and interaction with the big display

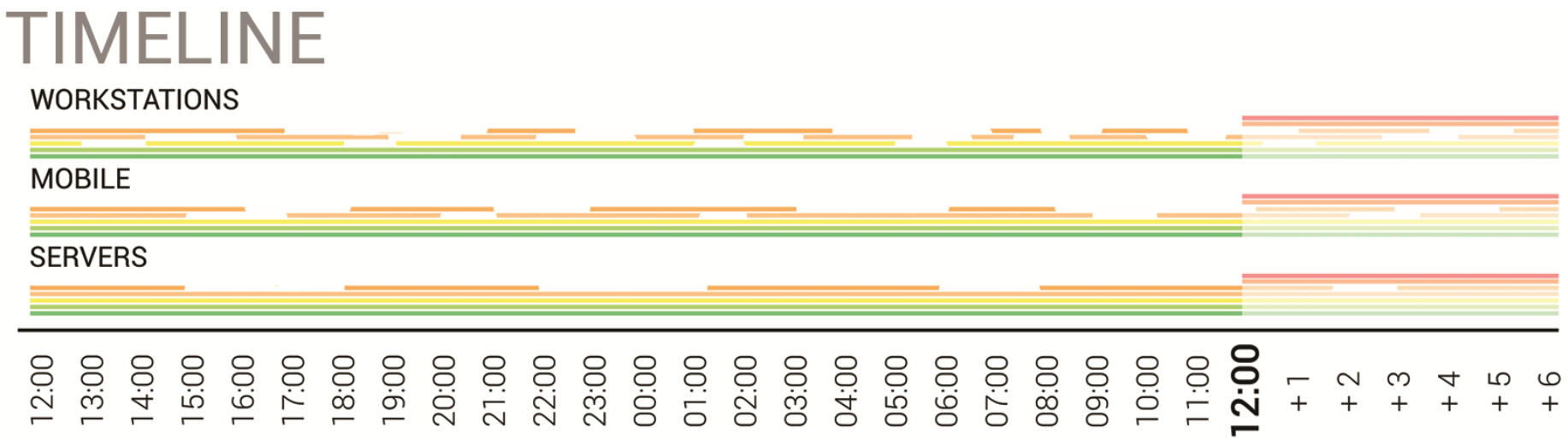




CALME stands for Cyber AnaLysis & Monitoring Environment (CALME). CALME is designed to aide in the monitoring network assets and infrastructure to support rapid response for security incidents and network degradation as well as help with planning tasks.



Concern Level Assessment (CLA) view. The Concern Level Assessment is a six-level variable which aggregates a range of indicators from individual assets. The indicators were established previously by Middlesex University through interviews with network security experts as providing indication of concern they would have for individual assets given a range of indicative variables. In the Concern Level Assessment view these are aggregated across assets to provide a view of the health of the network as a whole.



Timeline view provide a history of what has been happening to the network over the previous 24 hours (CLA status). It also displays predictions of the network state for the following six hours. It is envisioned that the Timeline view could also be used as a temporal control for the integrated view as a whole.

1st Oct 2013 @ 1200h

CRITICAL ISSUE

14 hrs 34 mins no issues

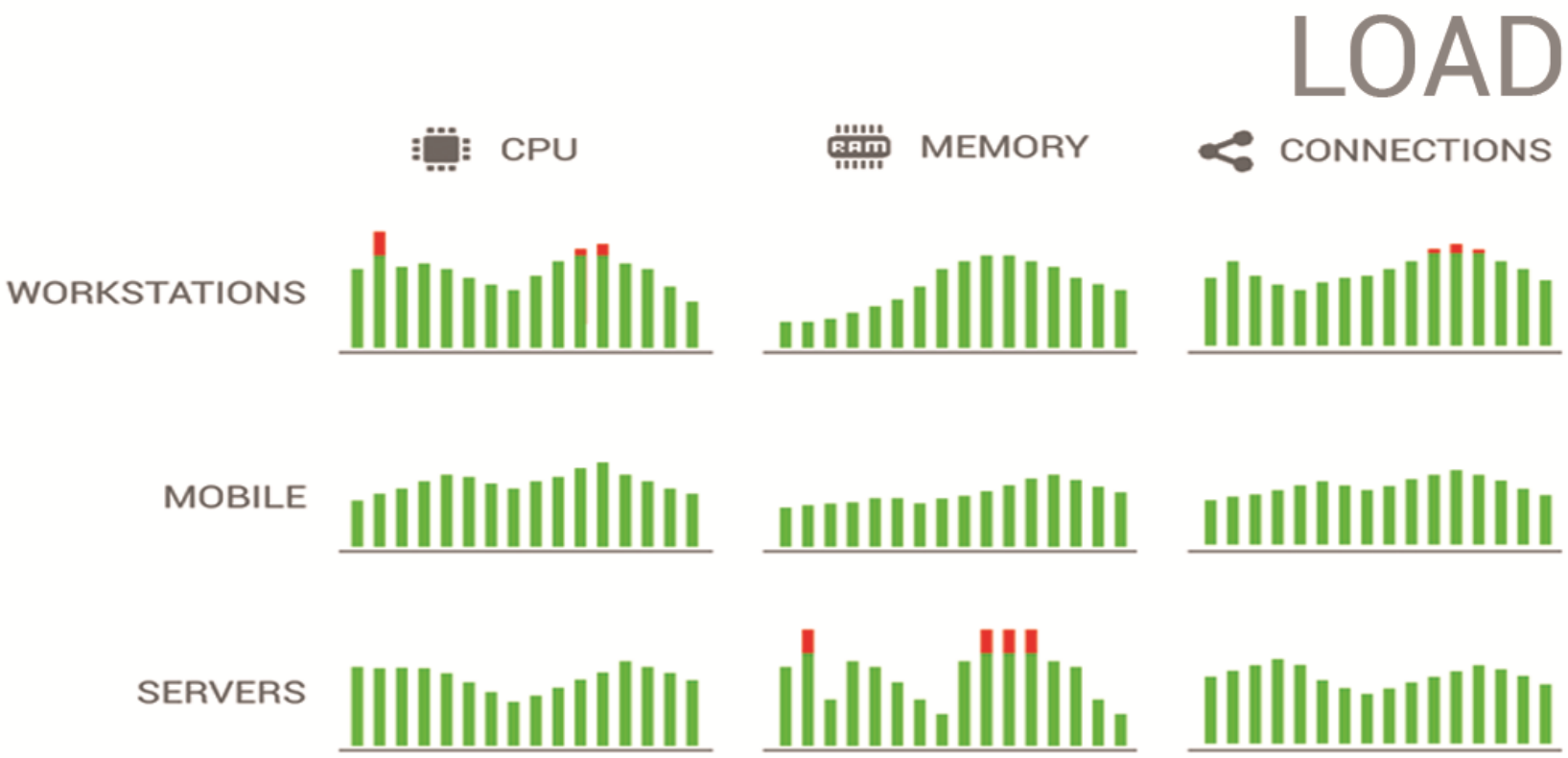
1st Oct 2013 @ 1600h

CRITICAL ISSUE

13:00

Not reporting - data centres and branches ...
- San Diego
- Los Angeles
- San Francisco

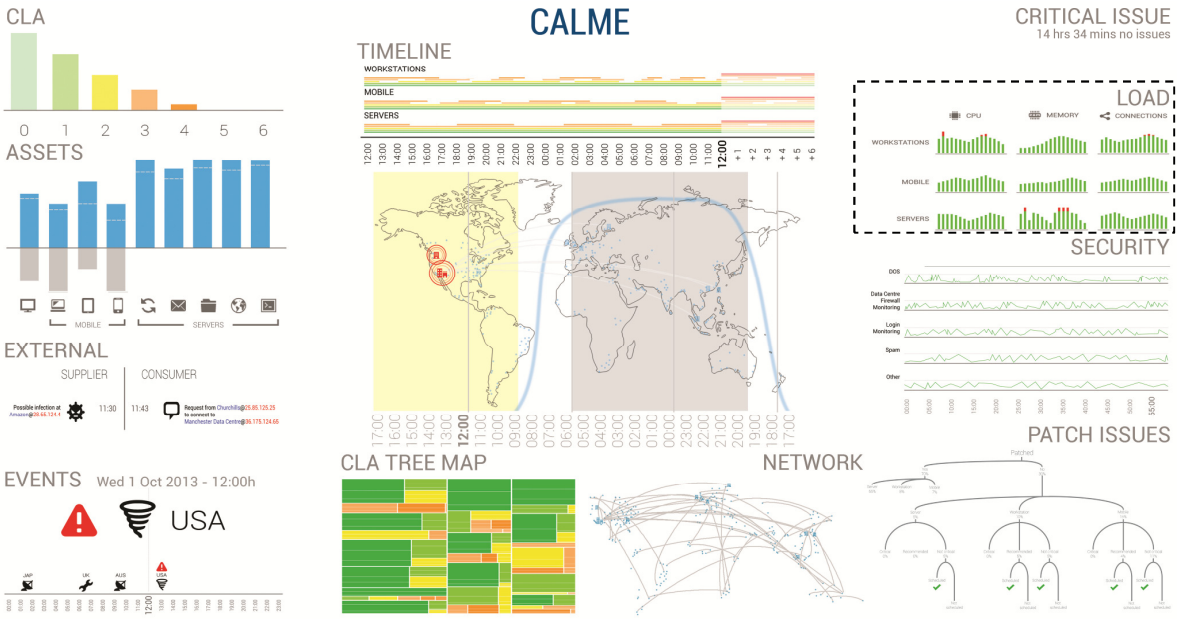
Critical issues view that under no issues circumstances displays how long it has been in that state but in the event of a critical issue, the issue is pinned on the view as a highlight.



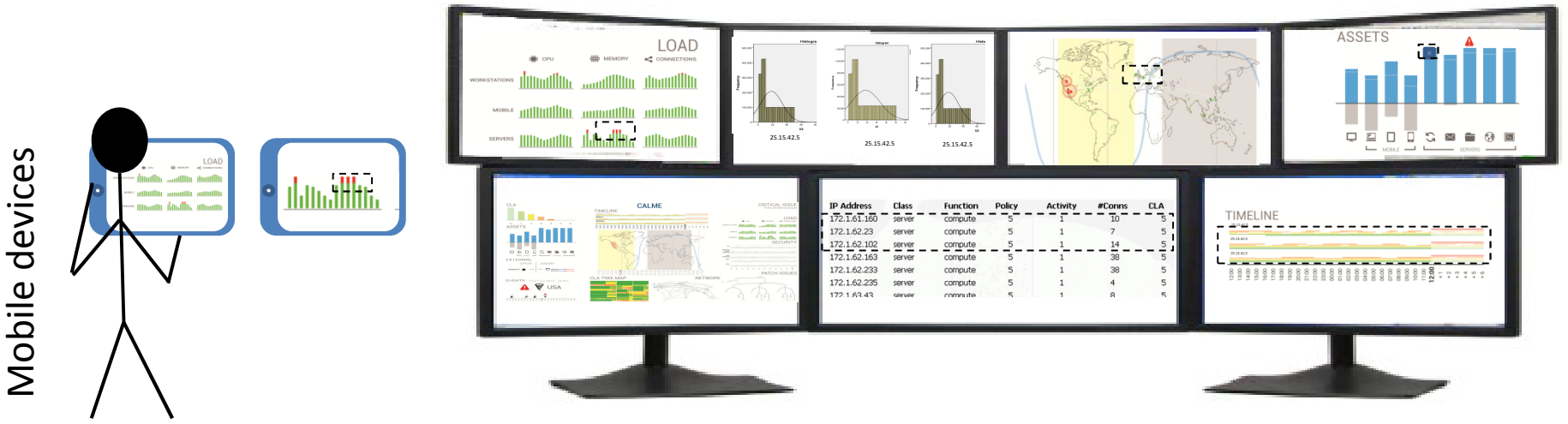
Load view that displays the overall network loads on assets, including cpu usage, memory usage and # of connections. It is envisioned that when fully implemented, this view will support a drill down that will allow the network operator to pin-point exact individual machines that are experiencing the high load.

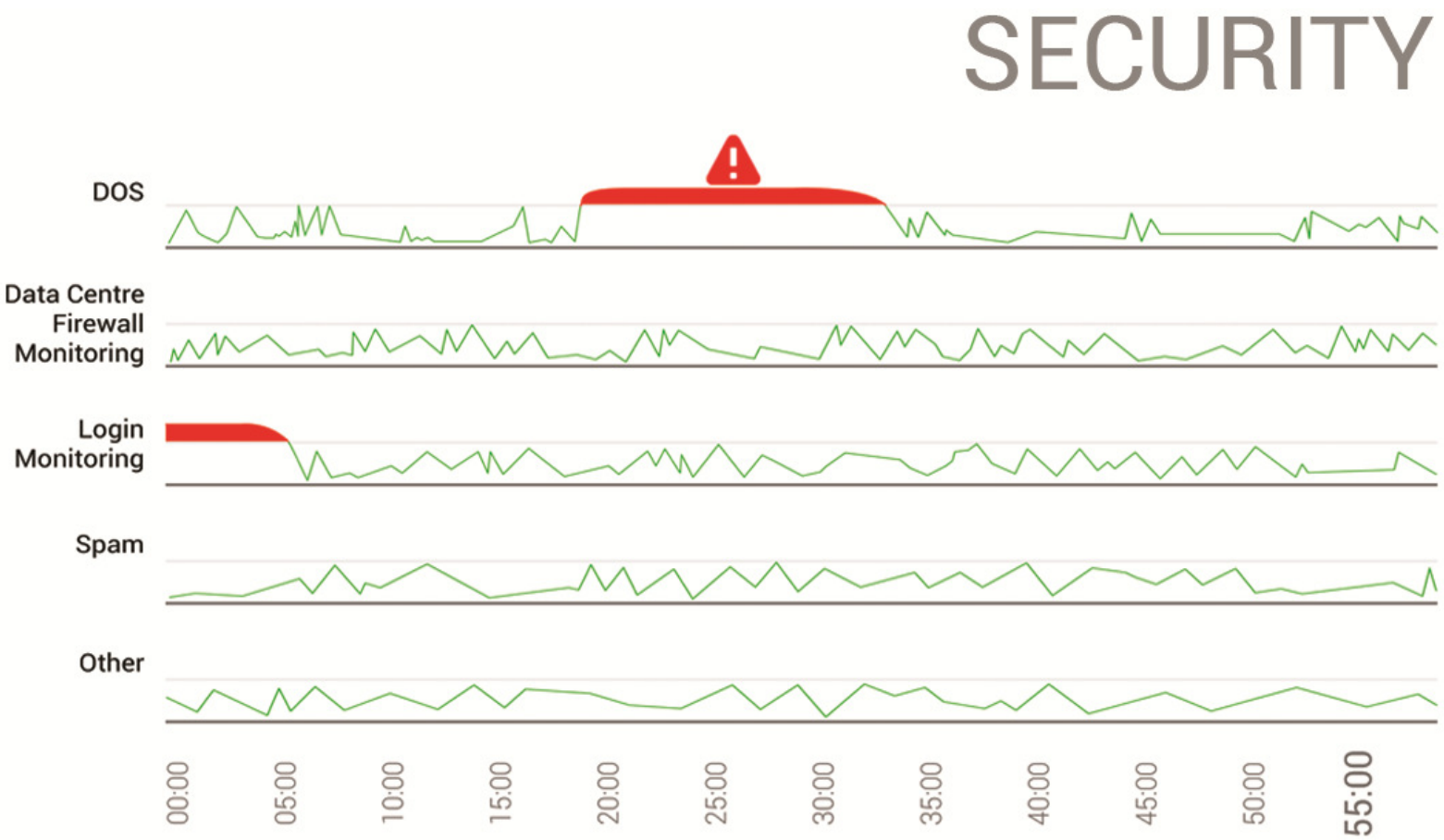
Situation awareness operation centre

Scenario 1: User holds a mobile device on to the CALME situation awareness main display after observing few red spikes in the LOAD view. After zooming into the area of interest (on the mobile device) the user pass the information (gesture) onto an analyst to further drill down. The analyst is now able to explore machines which are related to the spike and where they are located and the machine type they belong to, along with detail level information of those machines, and finally how these machines status changed (CLA) over a 24 hour time.



Drill down and interaction with the big display – Load (mobile devices)

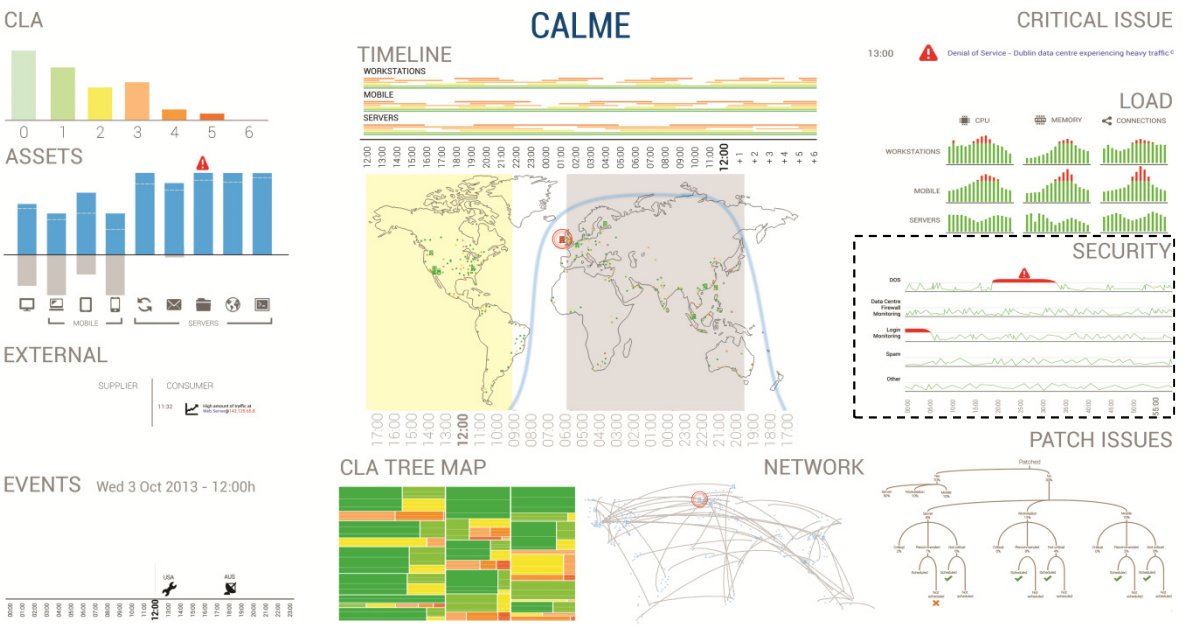




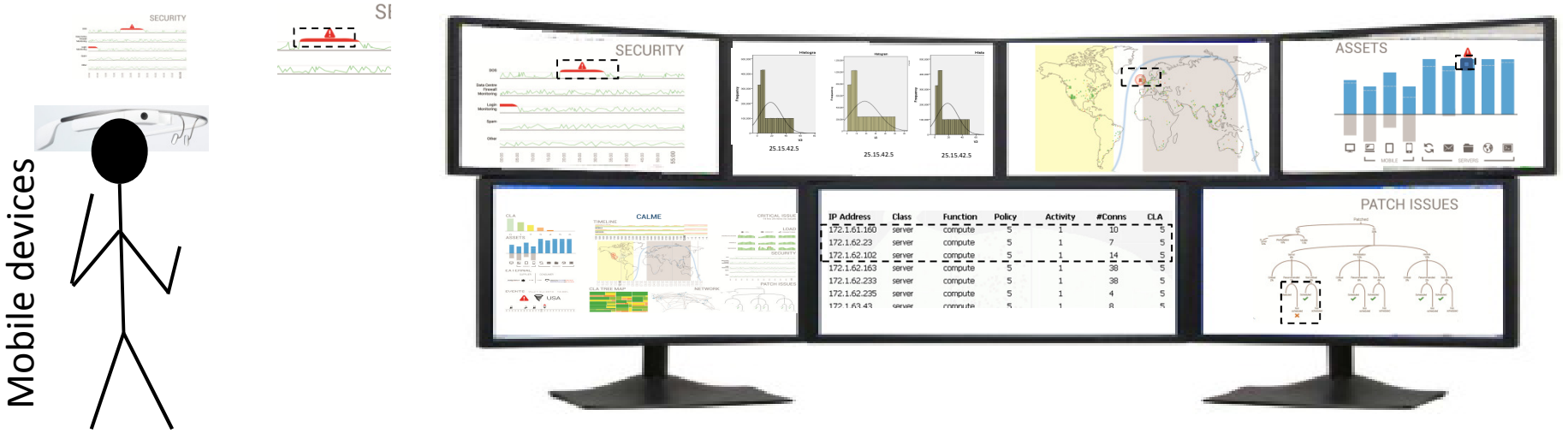
Security view that uses an ecg style visualisation to monitor security logs such as IDS and firewall logs but also to monitor administration login, login of accounts with high security clearance and access to sensitive information, as well as a monitoring when sensitive information is accessed.

Situation awareness operation centre

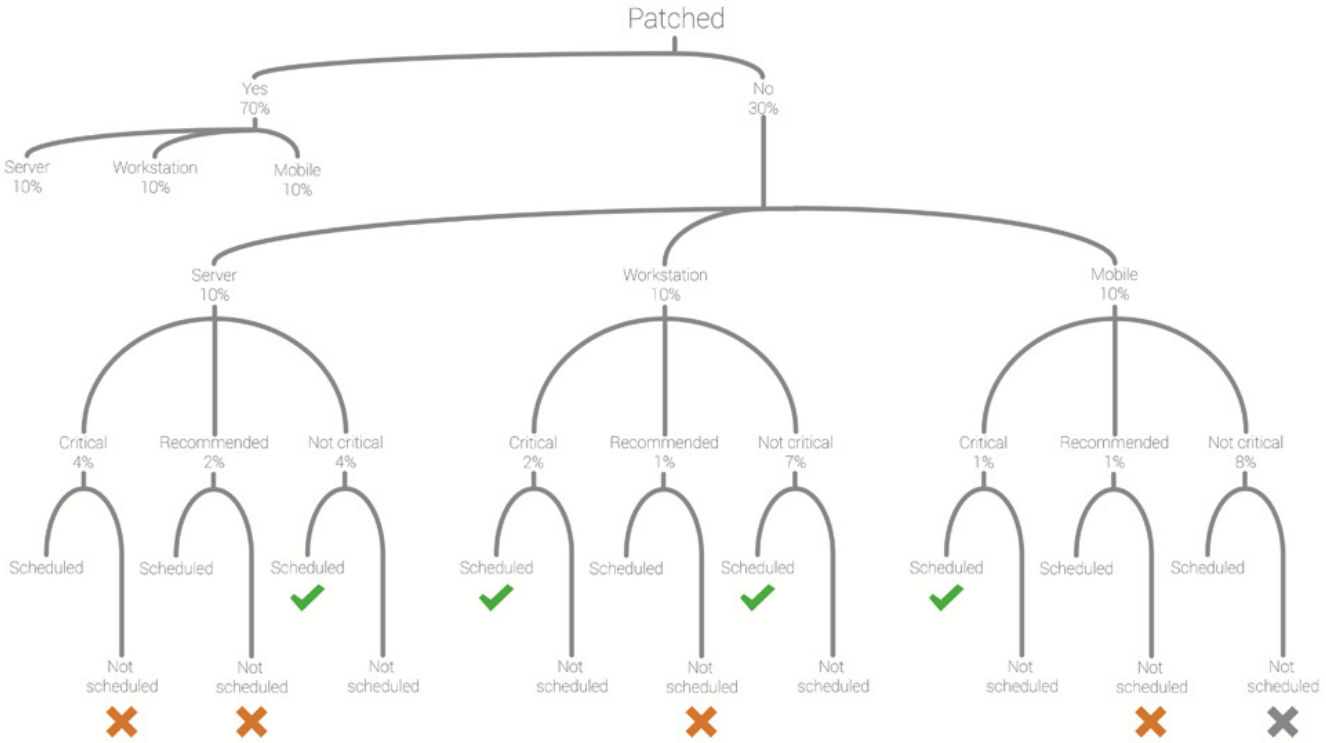
Scenario 2: User using wearable technology (e.g. Google glasses) after observing few red spikes in the SECURITY view. Similar to the previous, once the area of interest is selected, the user can passes the information to an analyst to explore further. The analyst is now able to explore machines which are related to the spike and where they are located and the machine type they belong to, along with further drill down level information of those machines, and finally if there was a relationship if patches had not been updated.



Drill down and interaction with the big display – Security (wearable technology)

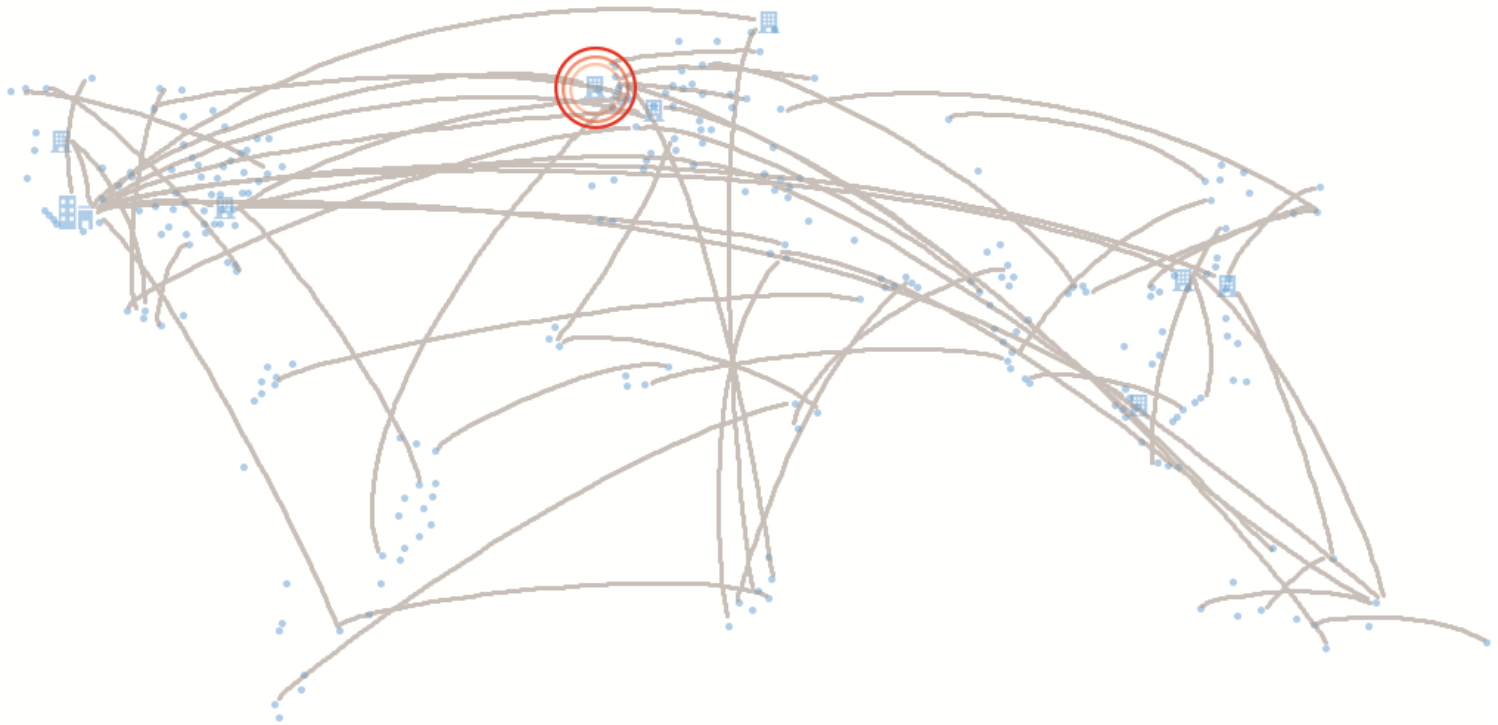


PATCH ISSUES



Patch monitoring tree that shows all unpatched machines, which patches are missing and whether the machine is scheduled to be patched or not.

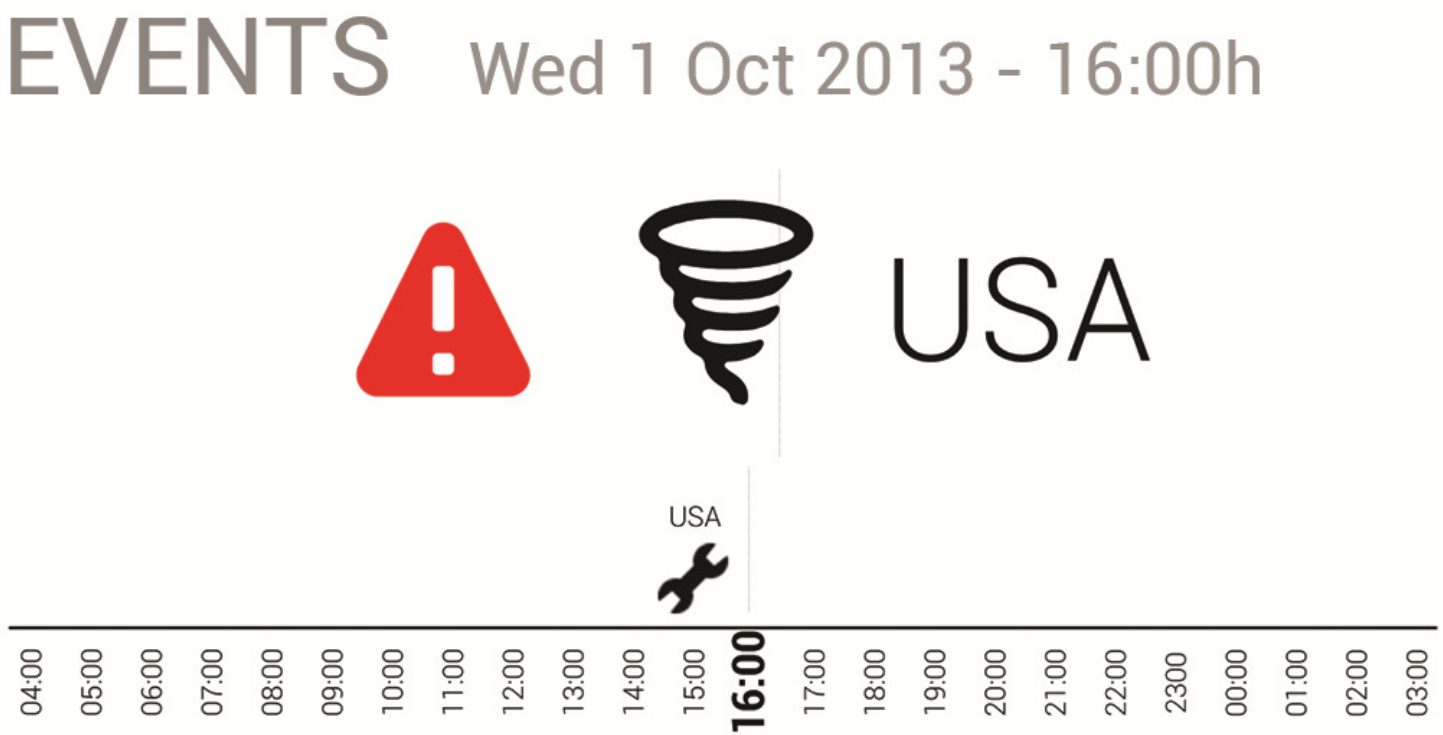
NETWORK



Network diagram that show the location of network switches, routers and any direct cable connections.

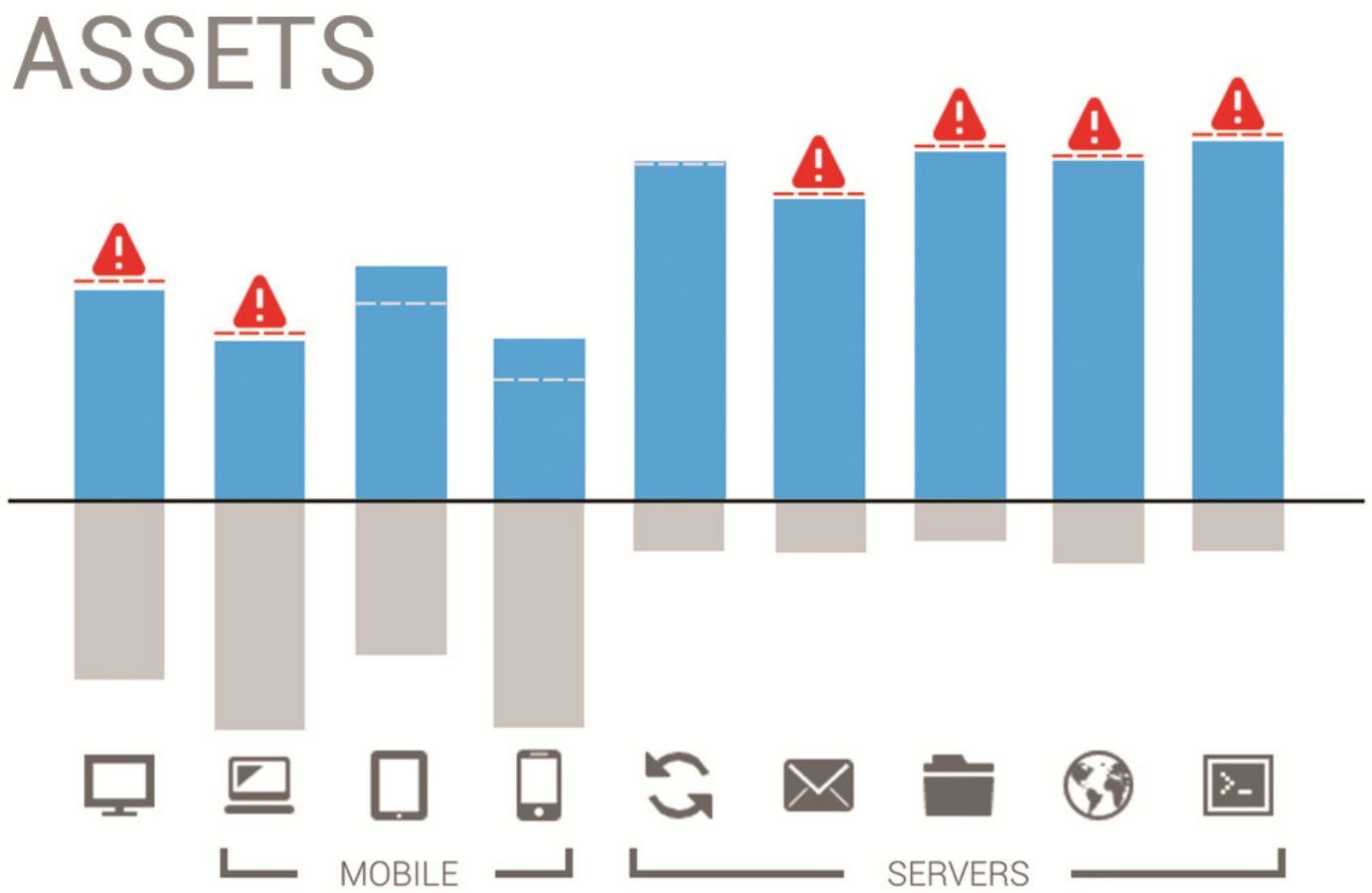
CLA TREE MAP

CLA Logic Map that distributes machines according to their CLA designation in a rough geographics format, divided according to regions with the top left hand corner roughly corresponding to North America and the bottom right hand corner corresponding to Australia and New Zealand.

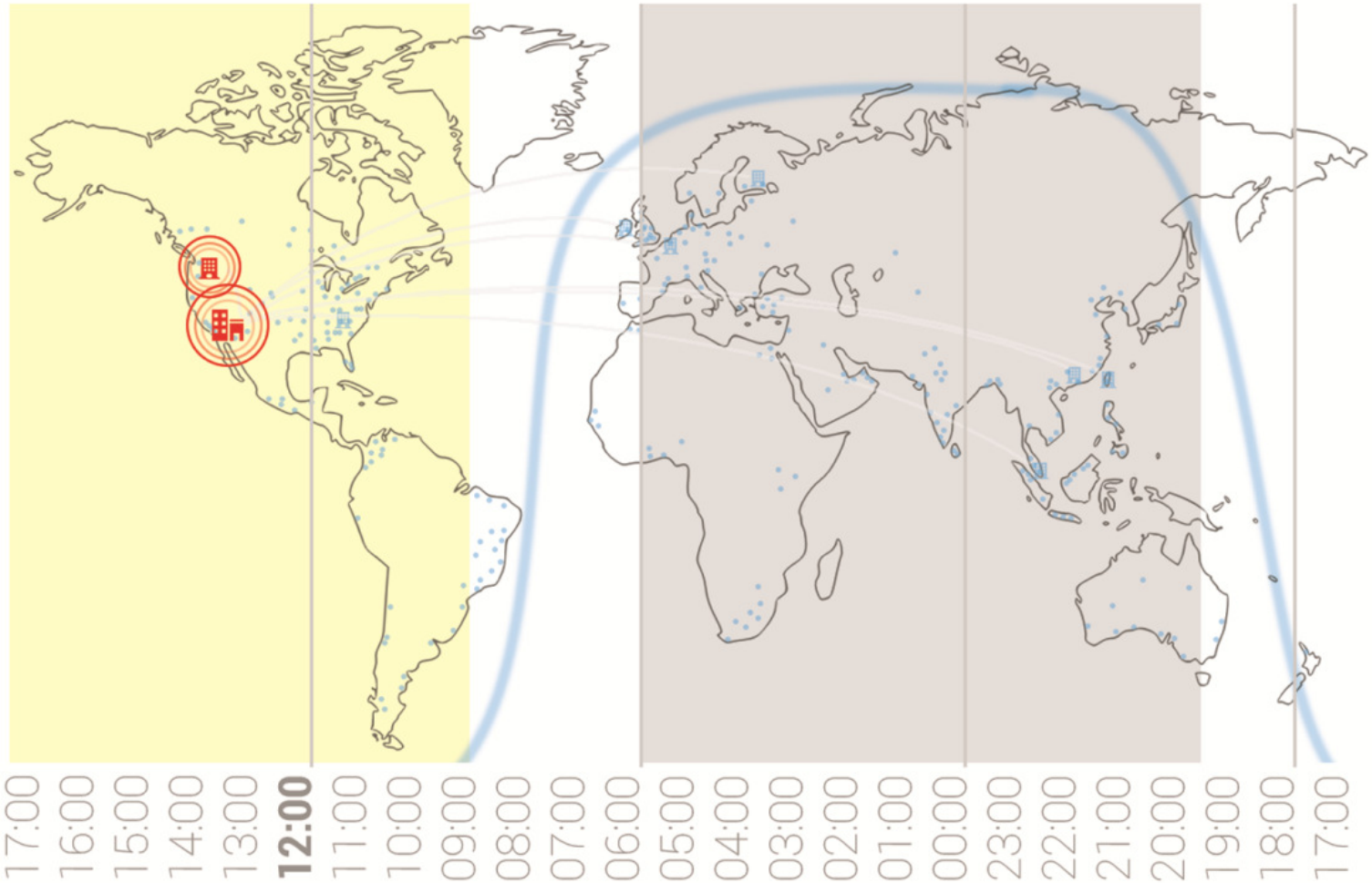


Event timeline that shows events that have past 12 hours in the past and events to come in the next 12 hours, including any events active at the current point in time. Events can be scheduled events such as maintenance or alerts from outside the organisation such as hurricane warnings.

Above the event view is the external supply chain monitoring which shows any events and alerts that are effecting suppliers and/or consumer.

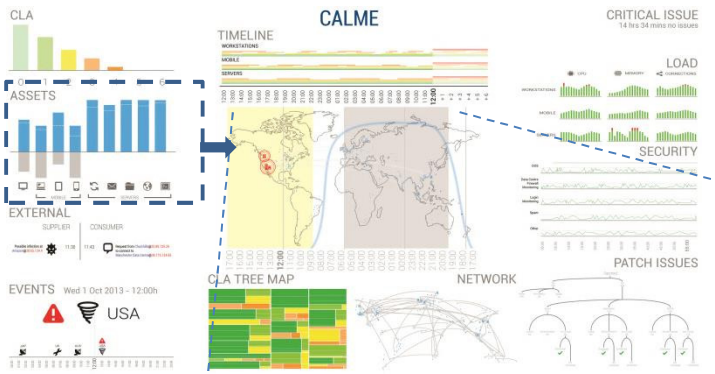


Asset view that gives one-glance overview of the state of the assets, divided according to their subclass of workstations, mobile devices and servers, with mobile devices and servers being further subdivided to paint a clearer picture. Assets in the blue portion of the bar chart are turned on and reporting, assets in the grey portion of the bar chart are not reporting and are either turned off or lacking network connection. The grey line indicate the seasonal norms. The red indicates when assets are abnormally below the seasonal norms.



Map view, which gives the geolocation of all the assets. This map view can be altered to by pinching parameters that are by default shown on the views surrounding the central map and dropping it on the map view.

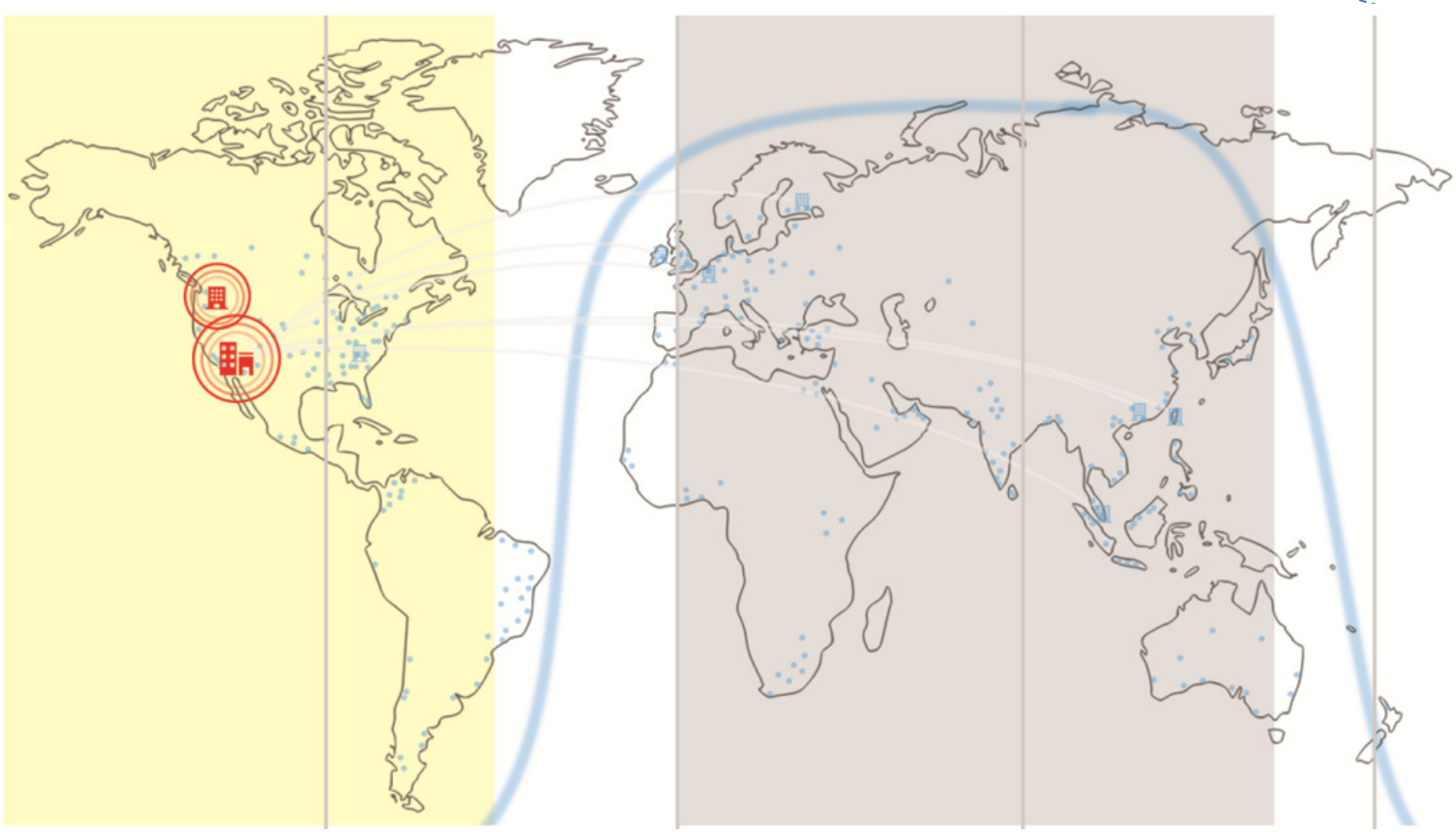
Pinch and drop views onto the map – Default to CLA

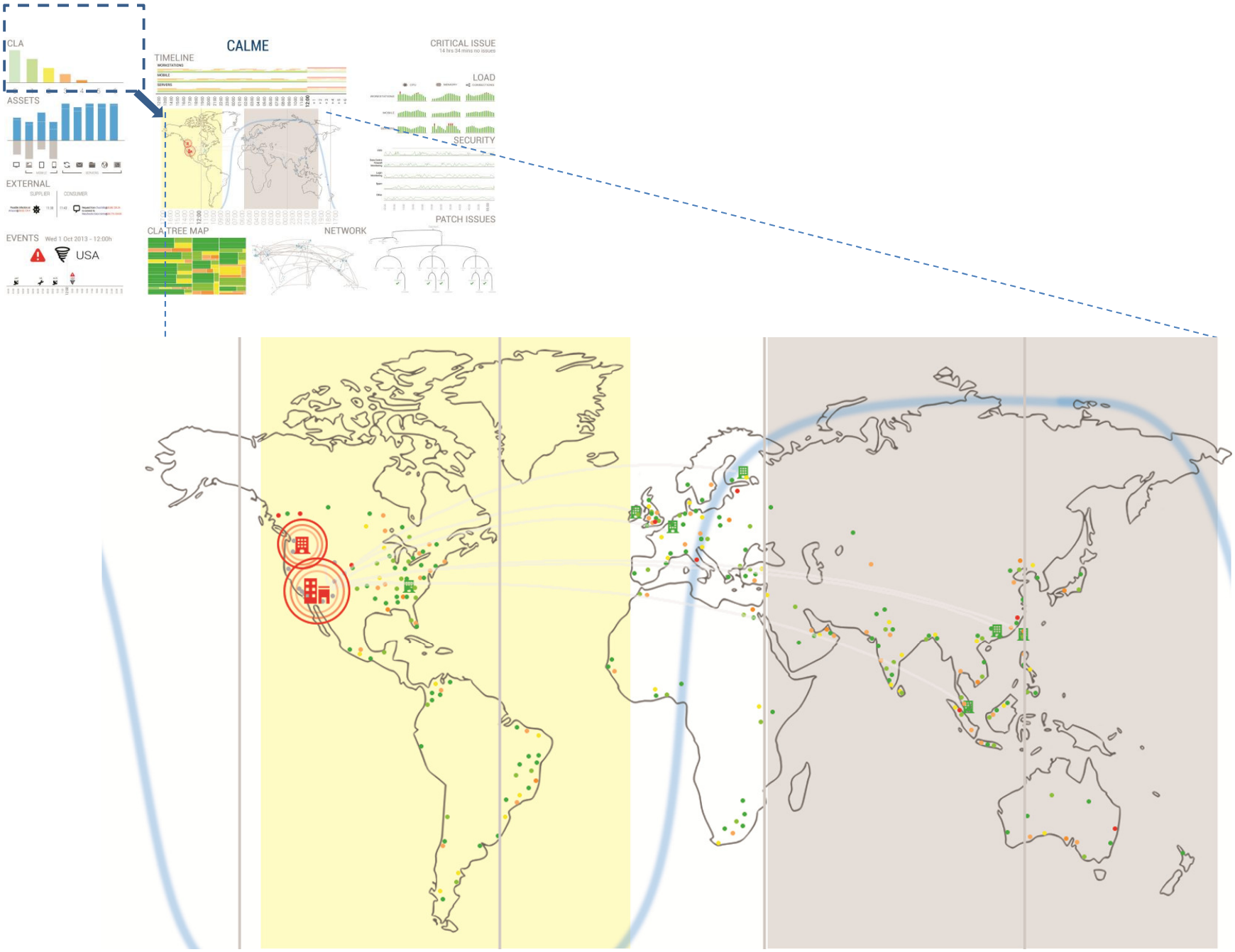


Scenario 3: CALME by default shows assets which are reporting over the network from facilities (such as: head quarters, data centers, branches etc).

Users are able to pinch and drop a view (e.g. CLA) on to the map to observe how the CLA is distributed across the assets in the facilities. The highest reporting CLA of a facility is reported onto the map to avoid clutter.

Similarly pinch and drop could be achieved with critical issues (identify geolocation of issues), load view (where spikes occur), etc.




CLA
ASSETS
EXTERNAL
SUPPLIER
CONSUMER
EVENTS
Wed 1 Oct 2013 - 12:00h
USA
CALME
TIMELINE
CRITICAL ISSUE
14 hrs 34 mins no issues
LOAD
SECURITY
PATCH ISSUES
CLA TREE MAP
NETWORK