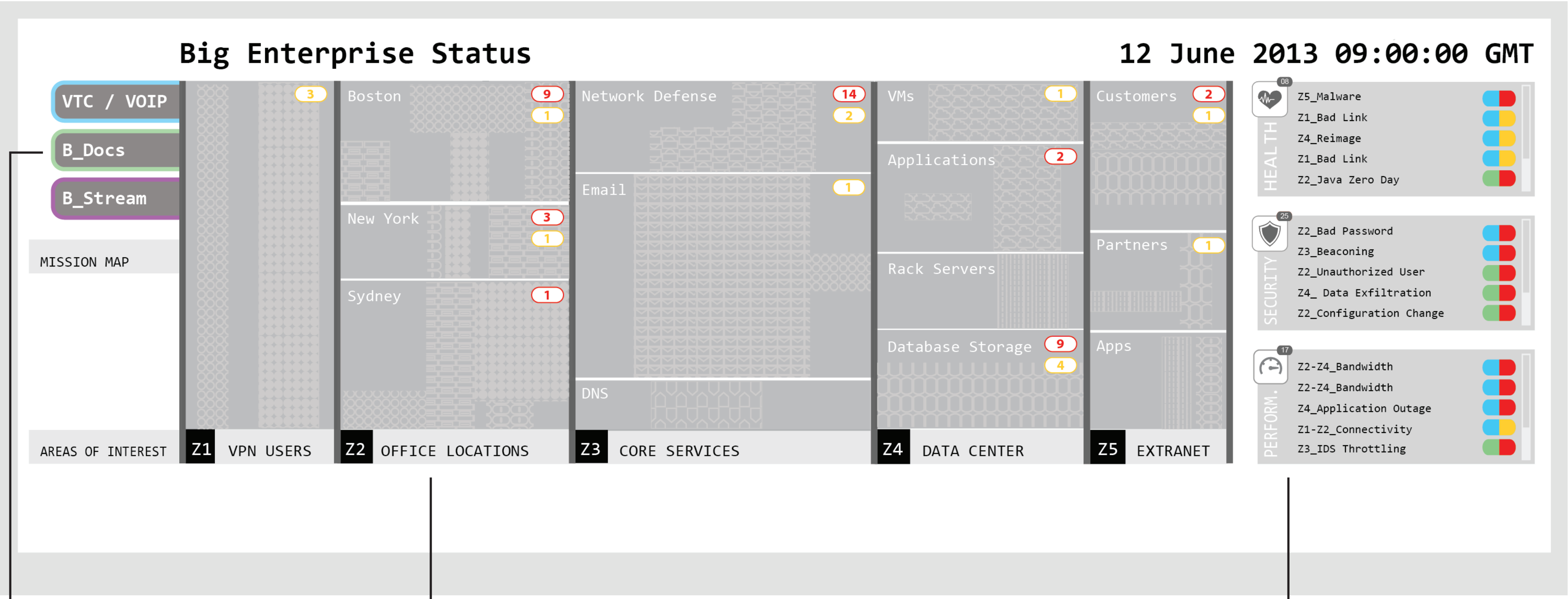
# Situational Awareness Display Design for VAST Challenge 2013

Diane Staheli, Andrea Brennen, David Danico, Raul Harnasch,
Maureen Hunter, Richard Larkin, Jeremy Mineweaser,
Kevin Nam, David O’Gwynn, Harry Phan, Alexia Schulz,
Michael Snyder, Tamara Yu

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

This work is sponsored by the Assistant Secretary of Defense under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government.



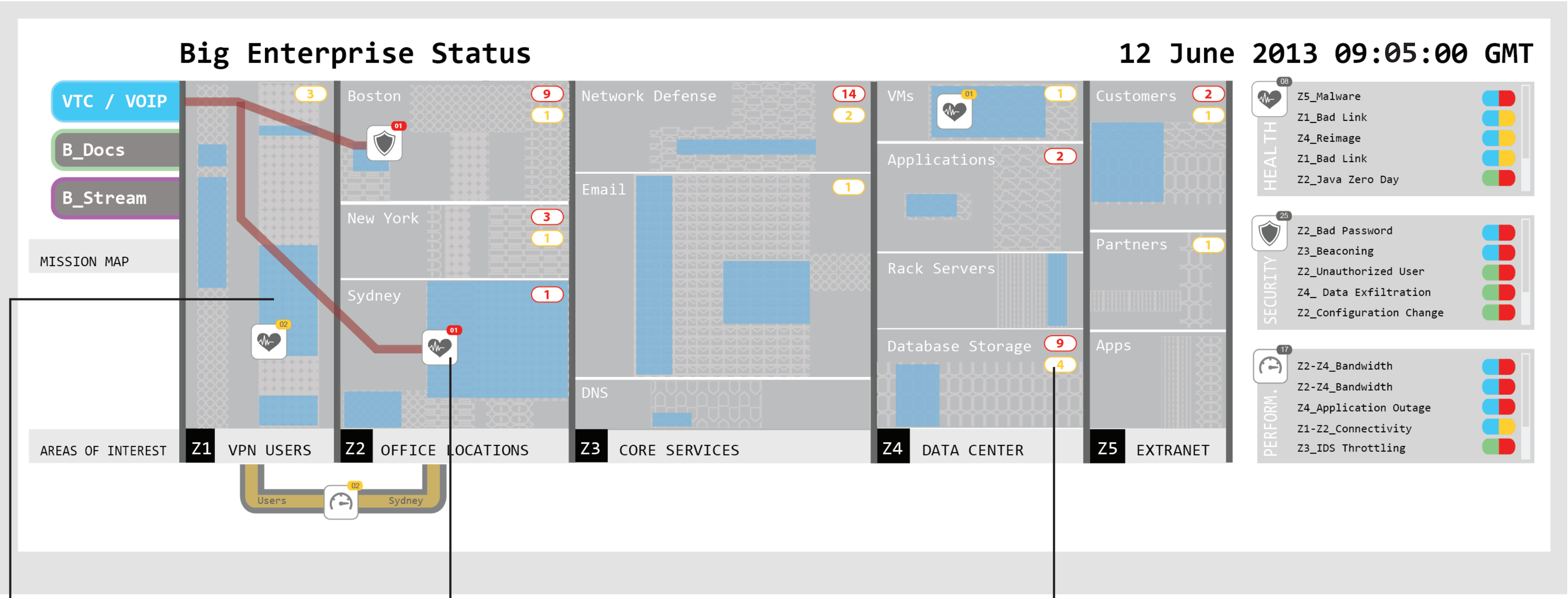
*A NOC manager can filter the display to see resource use and warnings per "mission area."*

*The B.E. BigBoard provides a high-level overview of the Big Enterprise Network. The display shows resource allocation across various enterprise functions (divided into five "zones").*

*The "Warning Menu" displays all current health, security, and performance issues.*

Big Enterprise or B.E. is a multibillion dollar telecommunications and virtual services company. Their offices and data centers offer cloud storage, streaming media for training, Video Teleconferencing, and Voice Over IP for companies all over the world. It is the responsibility of the Network Operation Center to maintain service availability by managing many types of network related issues, ranging from network intrusions to bandwidth allocation.

The B.E. Solution for situational awareness is an interactive display designed to provide a concise visual representation of the state of the Big Enterprise network.  The goal of the display is to facilitate the prioritization of network problems as they arise, by explicitly depicting how problems interrelate.  The board depicts how network problems are geographically or functionally distributed and illustrates how they impact critical enterprise mission areas.



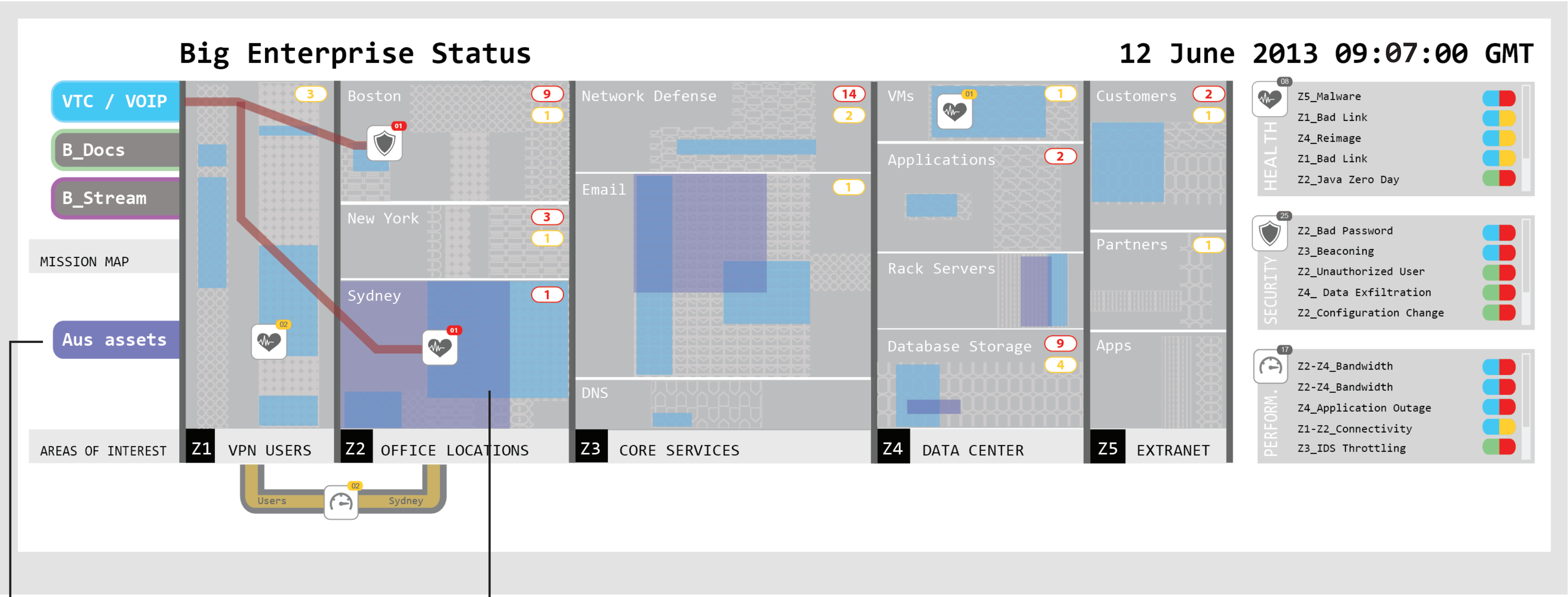
*Enterprise resources allocated to VTC / VOIP are shown in blue.*

*Warning icons indicate problems pertaining to the highlighted "mission area."*

*Warning bubbles show the total number of issues per function or geographic area. New issues are shown in red; yellow indicated an issues is actively being addressed.*

In this example, the NOC Manager can go through each mission area to check on health, security, and performance, making sure all issues are addressed. Here enterprise resources pertaining to the day-to-day function of the VTC/VOIP mission area are highlighted in blue across all zones. When specific problems arise, warning icons appear on the board indicating the type of issue, be it health, security or performance, which functional zone the issue impacts, as well as the status of the problem: new problems are shown in red, and yellow indicates an issue is currently being worked. Bubbles at the top right summarize the number of events in each area, and update depending upon the mission currently being viewed. The aggregation of events simplifies the view of healthy systems, while the pop-up notifications draw attention to portions of the network that require immediate action.

A complete summary of all warnings is on the far right side of the board; each warning is categorized by the three types and labeled by zone. A pill icon indicates which mission the issue impacts the most and whether the issue is being addressed.



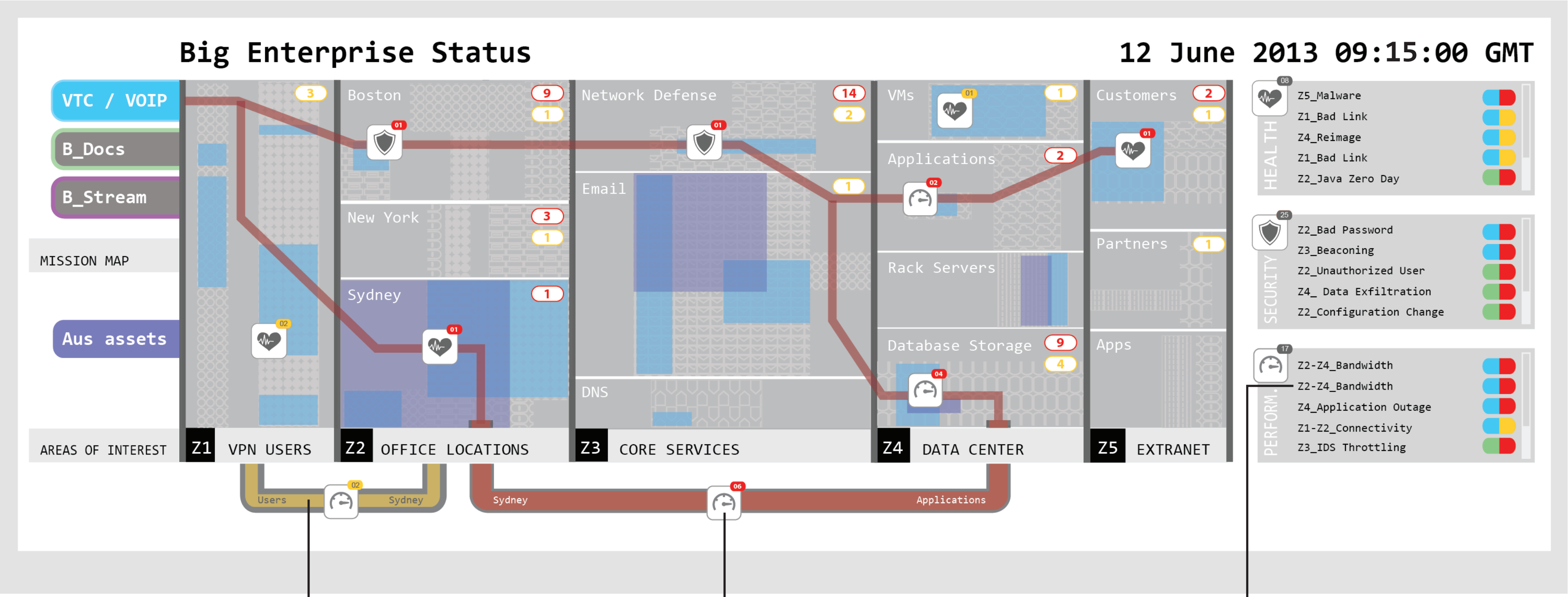
*The BigBoard accommodates custom searches for both geographic and functional queries*

*A search returns a "mapping" of relevant allocated or impacted enterprise resources.*

---

One adaptable feature of the BigBoard that aids situational awareness is a search tool with the flexibility to highlight geographic and functional categories based upon user input.

Here, the NOC manager sees a decrease in traffic (shown by the yellow pipe) between Zone 1 and Zone 2. She wonders if it is because Sydney is shutting down as part of their cyclone preparations. Searching for Assets in Australia displays a lower-than-normal density of resources being used by the Sydney office.



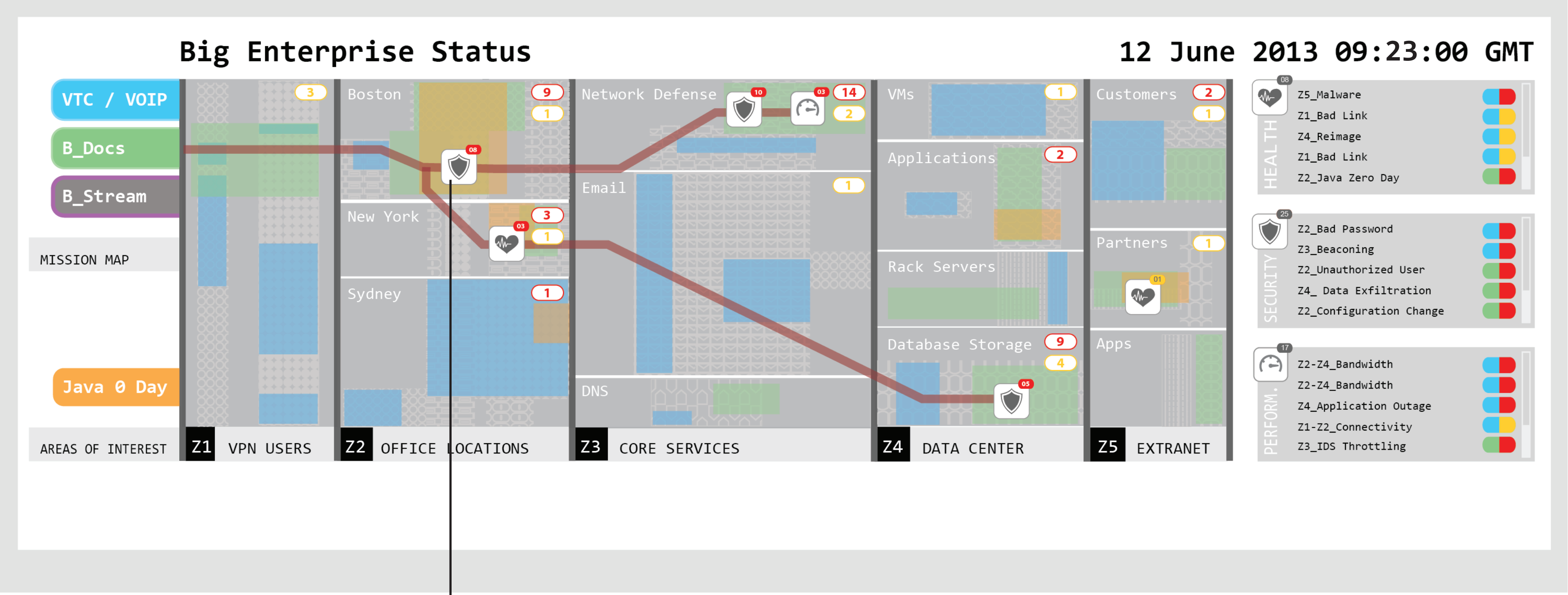
*"Pipes" give a qualitative indication of traffic flow between zones.*

*Icons continually appear on the Big-Board, indicating new issues.*

*Warnings are listed by zone and decribed with a keyword to help direct the right course of action.*

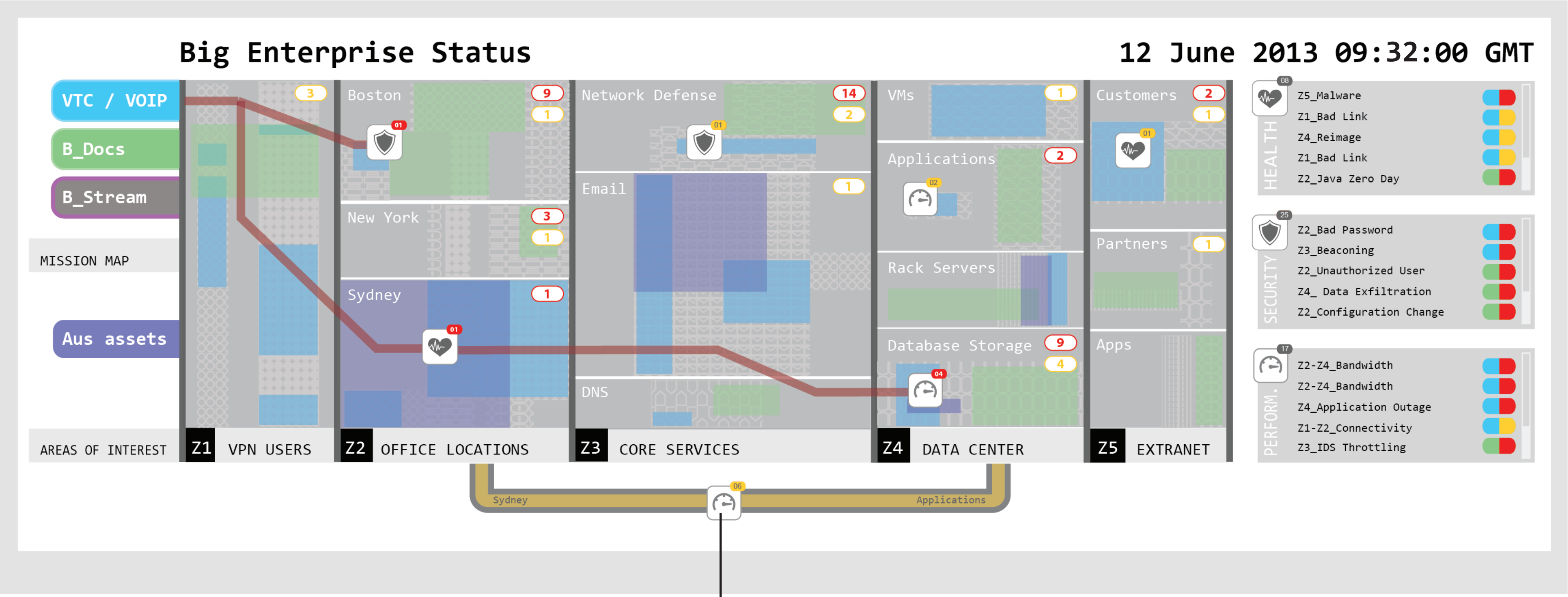
Before she can breathe a sigh of relief, the NOC manager notices traffic from Zone 2 to Zone 4 is increasing and starting to eat up bandwidth to the Data Center. Security badges in Network Defense indicate security issues, which in this case could be the result of beaconing. Performance badges appear in Applications and Data Storage, indicating outages and a Health badge appears in the Customers Zone, which she sees is likely the result of Malware.

Here, the NOC Manager learns from the Network Defense lead that root-kit activity leveraging a Java vulnerability is affecting B_Docs, the company's cloud storage service.



*A layering of different types of information shows how multiple functions are interrelated. Here, resources alloced to B_Docs (the content-sharing tool) are shown in green, unpatched machines are shown in orange, and a security warning icon indicates the presence of an "unauthorized user."*

Switching Mission views, the manager can do a search for vulnerable hosts. Sure enough, the root-kit is overlapping with unpatched machines. Apparently, as part of the cyclone preparations, Boston has been taking over Sydney's functions and some key machines were left unpatched. The Network Defense group quarantines the infected machines in Boston, blocking corresponding outbound traffic. However, they can't be shut down as they are filling in for functions diverted from Sydney.



*Warning icons turn yellow when they are in the process of being addressed and disappear when they are resolved.*

In the meantime, a number of badge icons previously in the VTC VOIP mission area have switched from red to yellow, indicating that that issues are actively being worked on, while other warnings have disappeared altogether, showing successful resolution.

In this scenario, the NETWORK OPERATIONS CENTER used the BigBoard to help B.E. avoid a potentially disastrous crisis. The network manager was able to use the display to gain situational awareness of the enterprise network where she could detect and prioritize issues, understand operational impact, and respond with the best course of action.