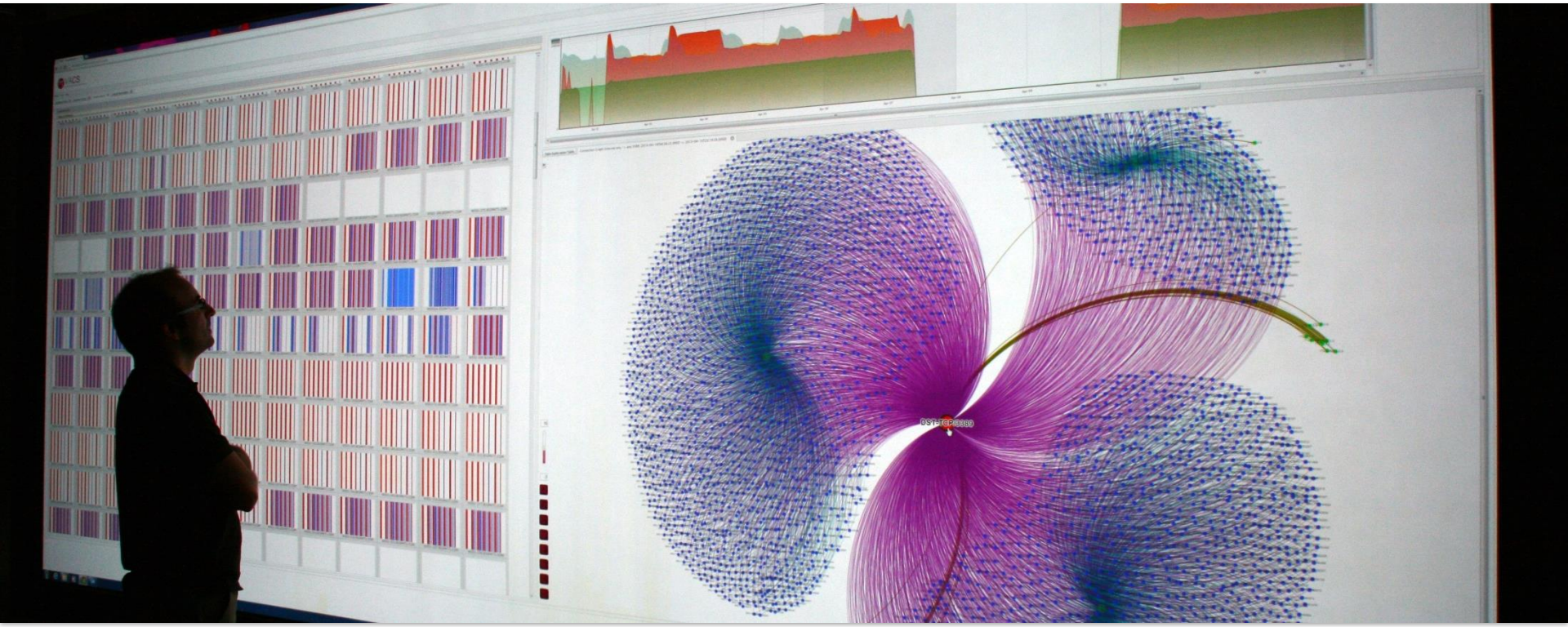
Universität
Konstanz



Visual Analytics Suite for Cyber Security (VACS): Visual Exploration of VAST Challenge 2013

Honorable Mention

Fabian Fischer and Daniel A. Keim

Data Analysis and Visualization Group | University of Konstanz

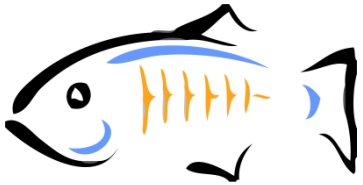
VIS-SENSE
www.vis-sense.eu

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257495.

Key Features

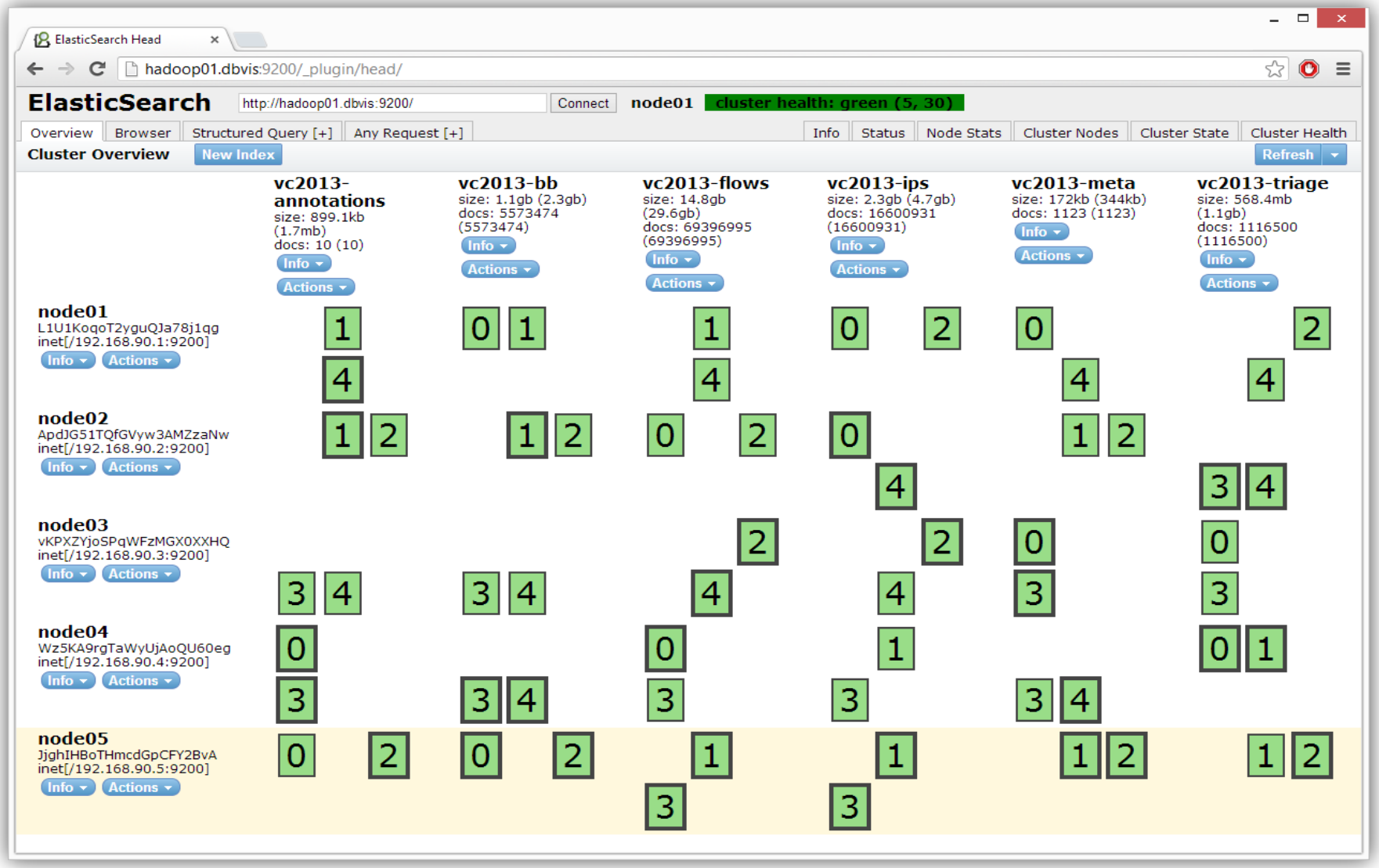
- **Backend:** Elasticsearch Cluster
  - Scalable Data Storage
  - Real-Time Queries
  - Date Histogram Facets

- **Server:** Java EE Application
  - Data Processing and Analysis
  - Server-Side Visualization Rendering

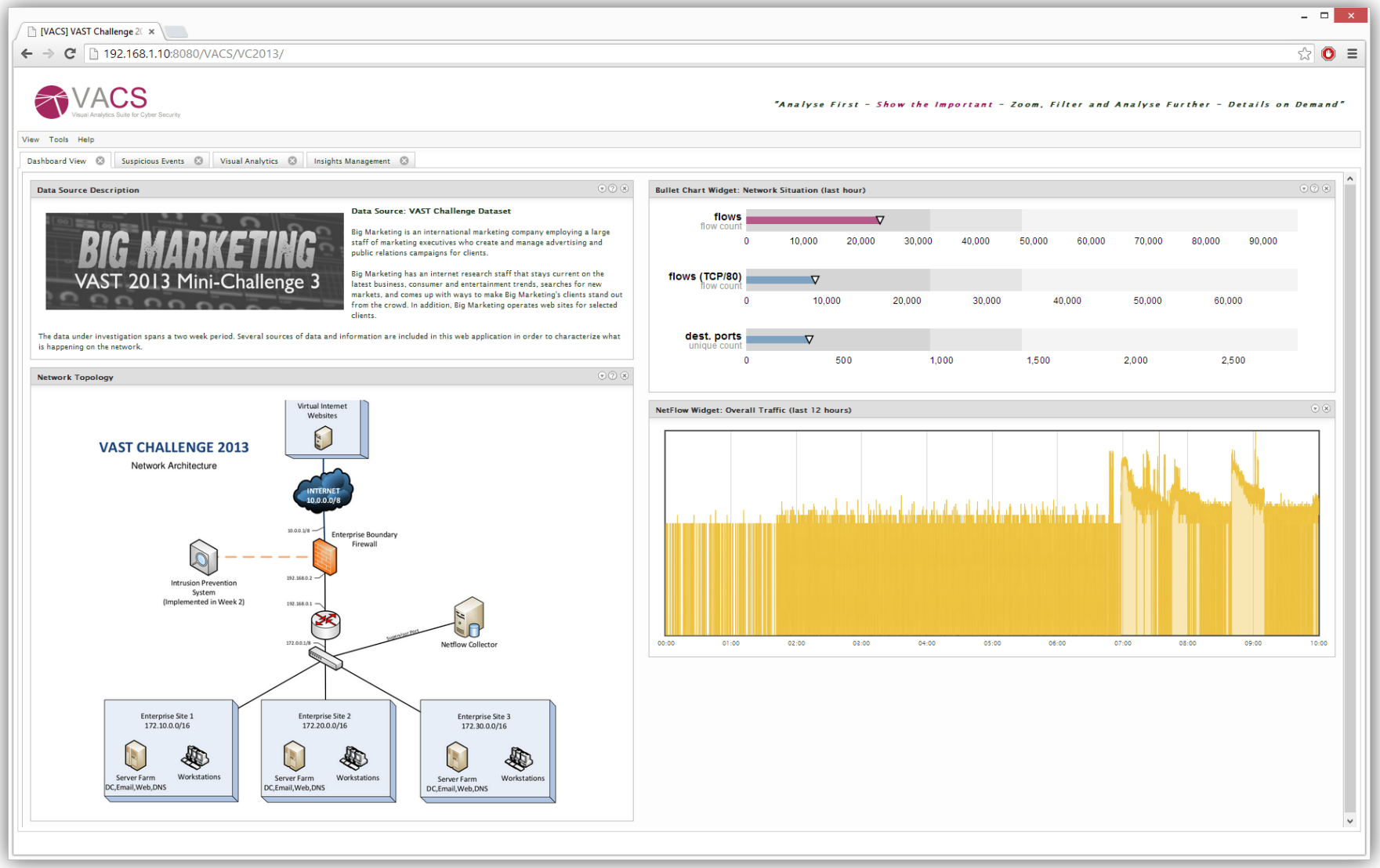


- **Client:** Web-Based JavaScript/HTML5
  - Visualizations (Static & Interactive)
  - Data Exchange via REST

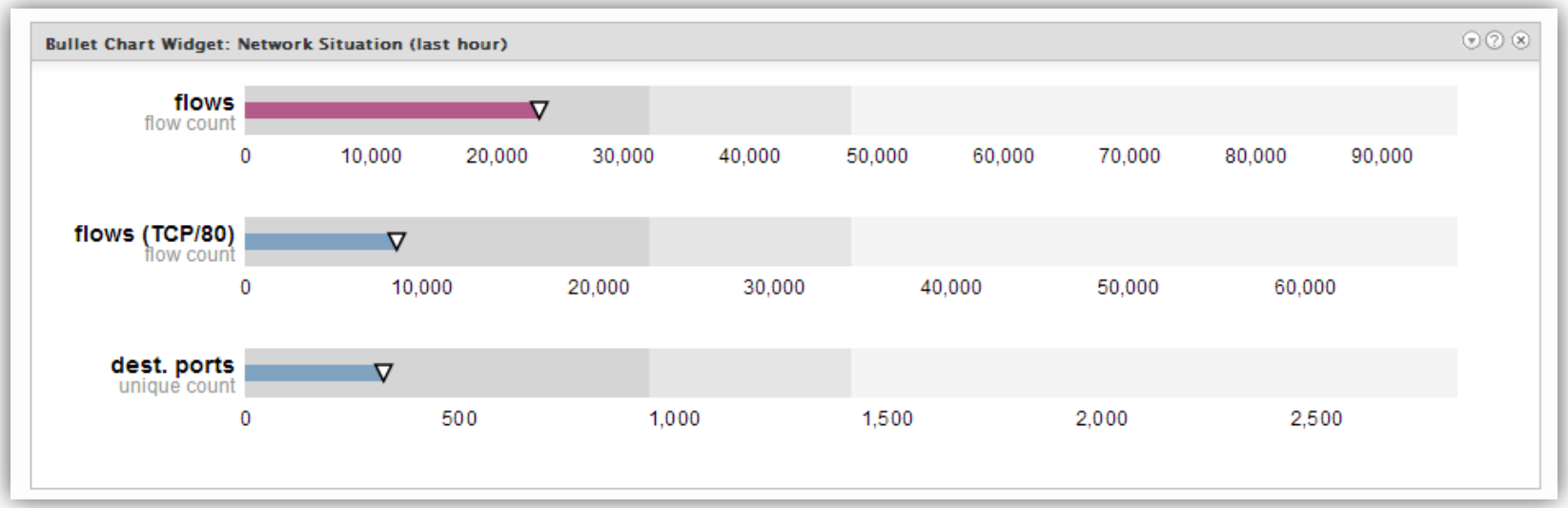
Backend: Scalable Elastic Search Cluster



Client: Real-Time Dashboard



Client: Bullet Chart Widget



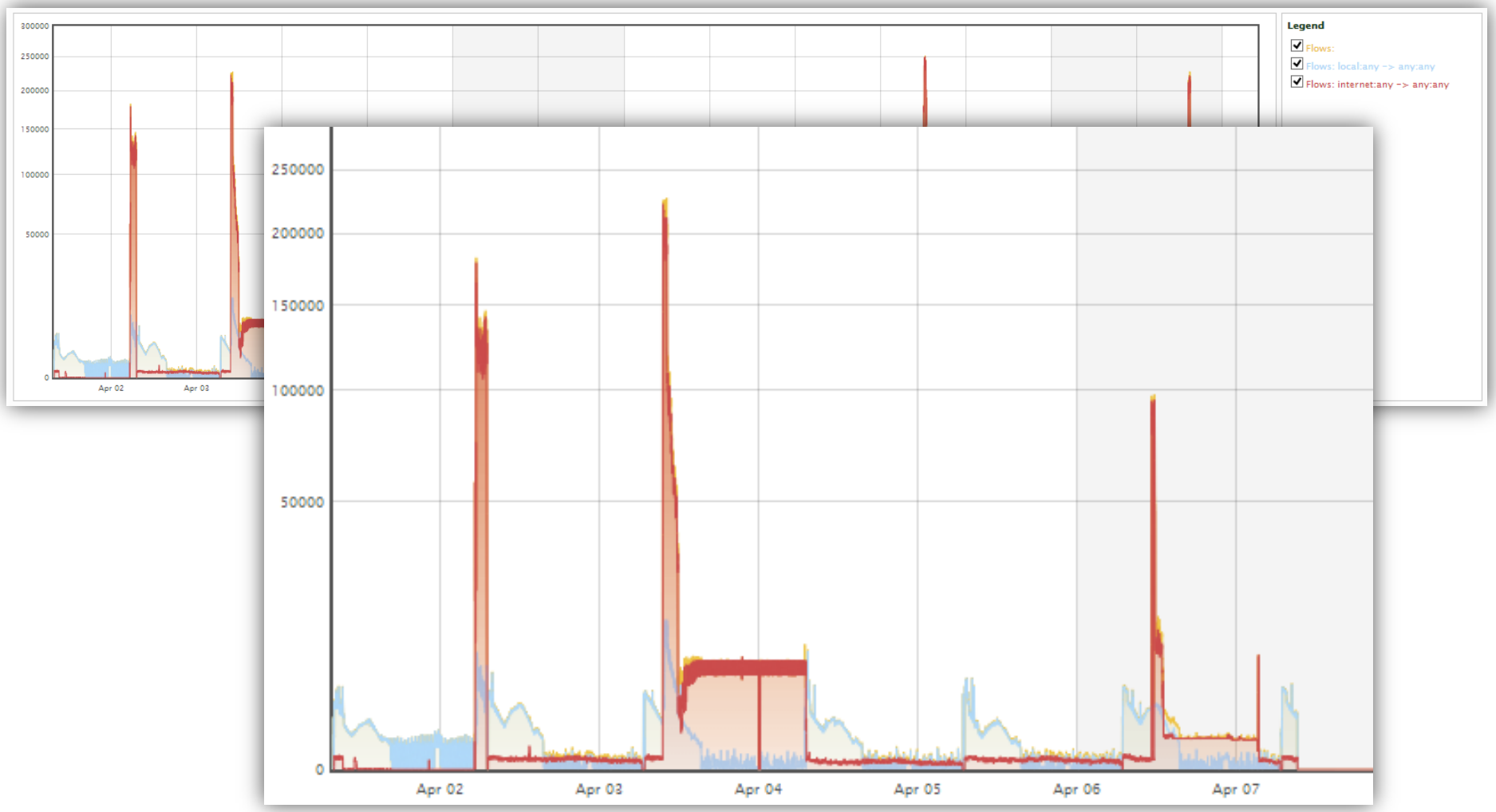
- Customizable widget for representing single measures in real-time dashboard.
- Set thresholds and ranges to highlight

Further Visual Exploration Possibilities

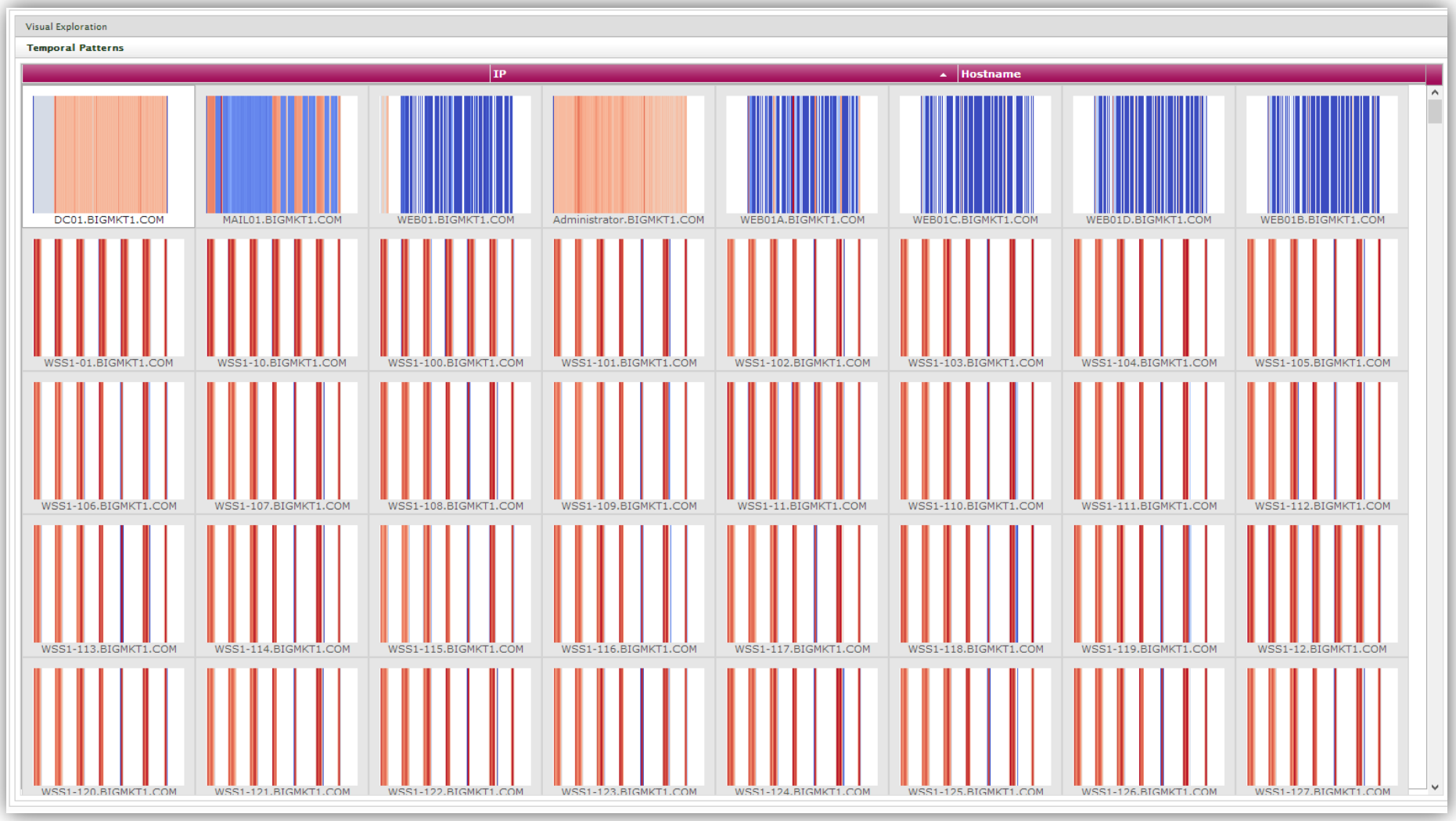
- **Interactive Line Charts**
  - Exploration and correlation of different data sources
- **Pixel-Based Thumbnails**
  - Identification of time-series patterns
- **TreeMap**
  - Usage overview of ports or hosts
- **Graph Viewer**
  - Exploration of network connections
- **Hierarchical ClockMap**
  - Time-Series patterns clustered with SAX[1]
- **Data Exploration Table**
  - Export raw data for further analysis

[1] Symbolic Aggregate approXimation

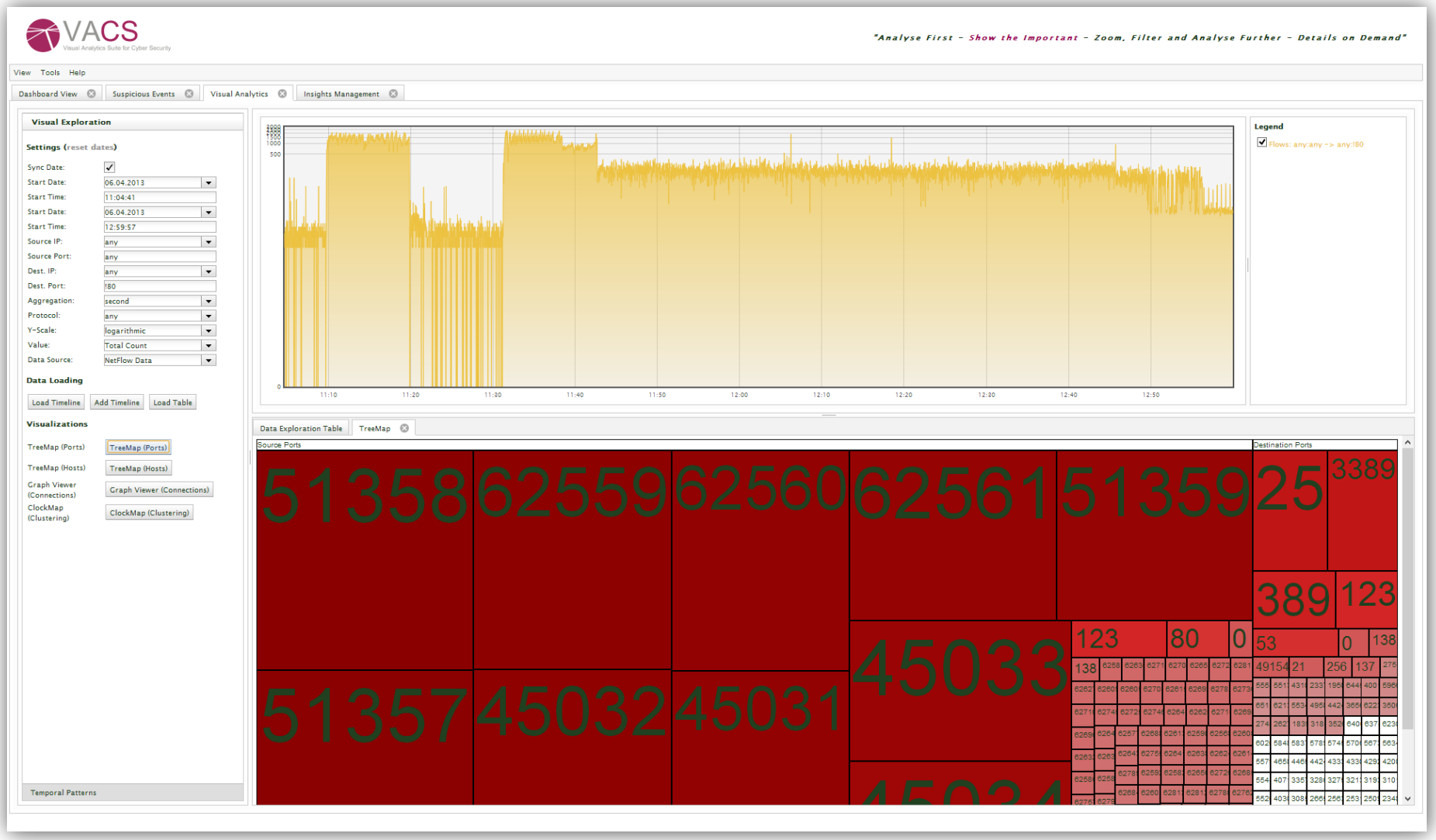
Interactive Line Charts



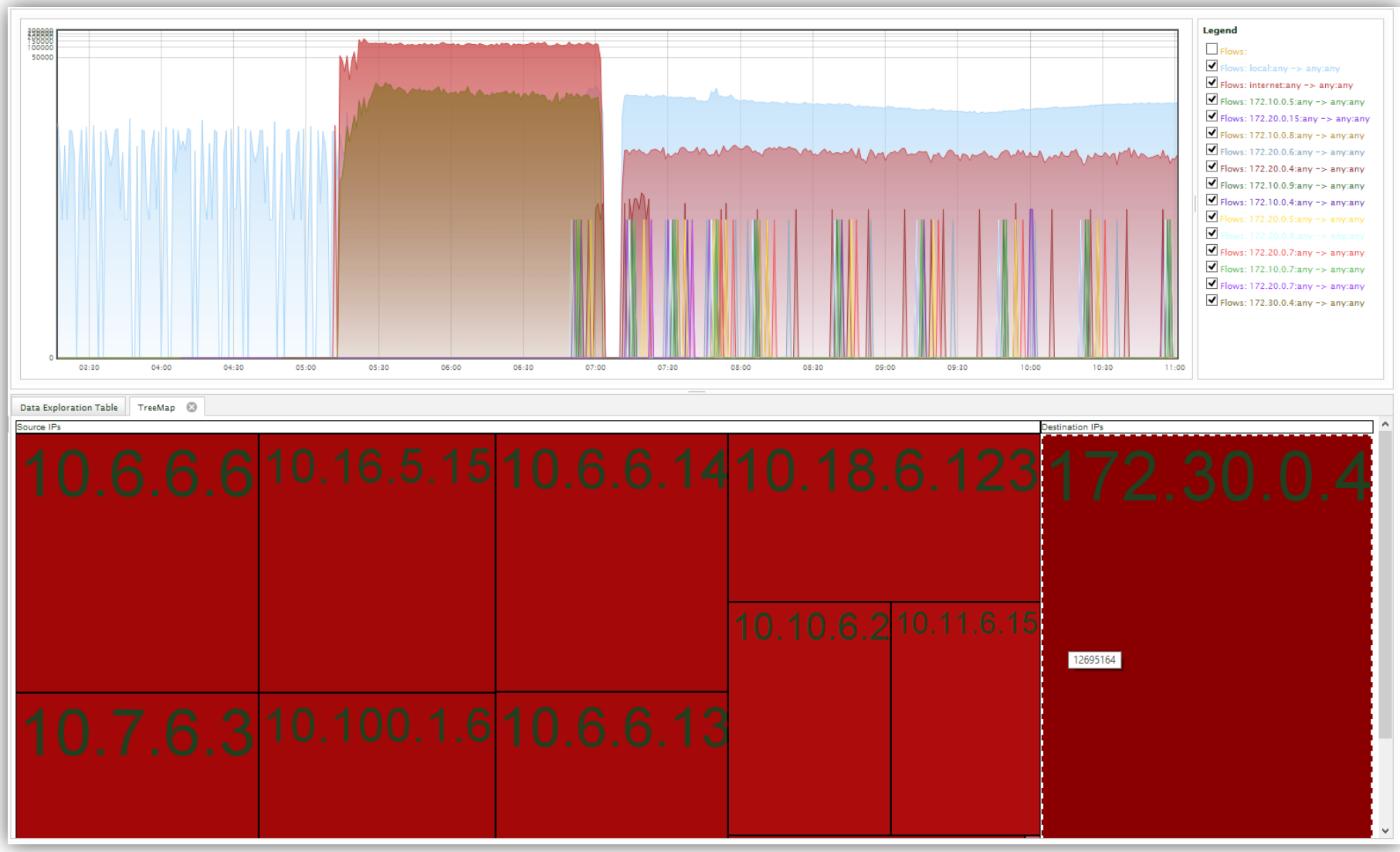
Pixel-Based Thumbnails



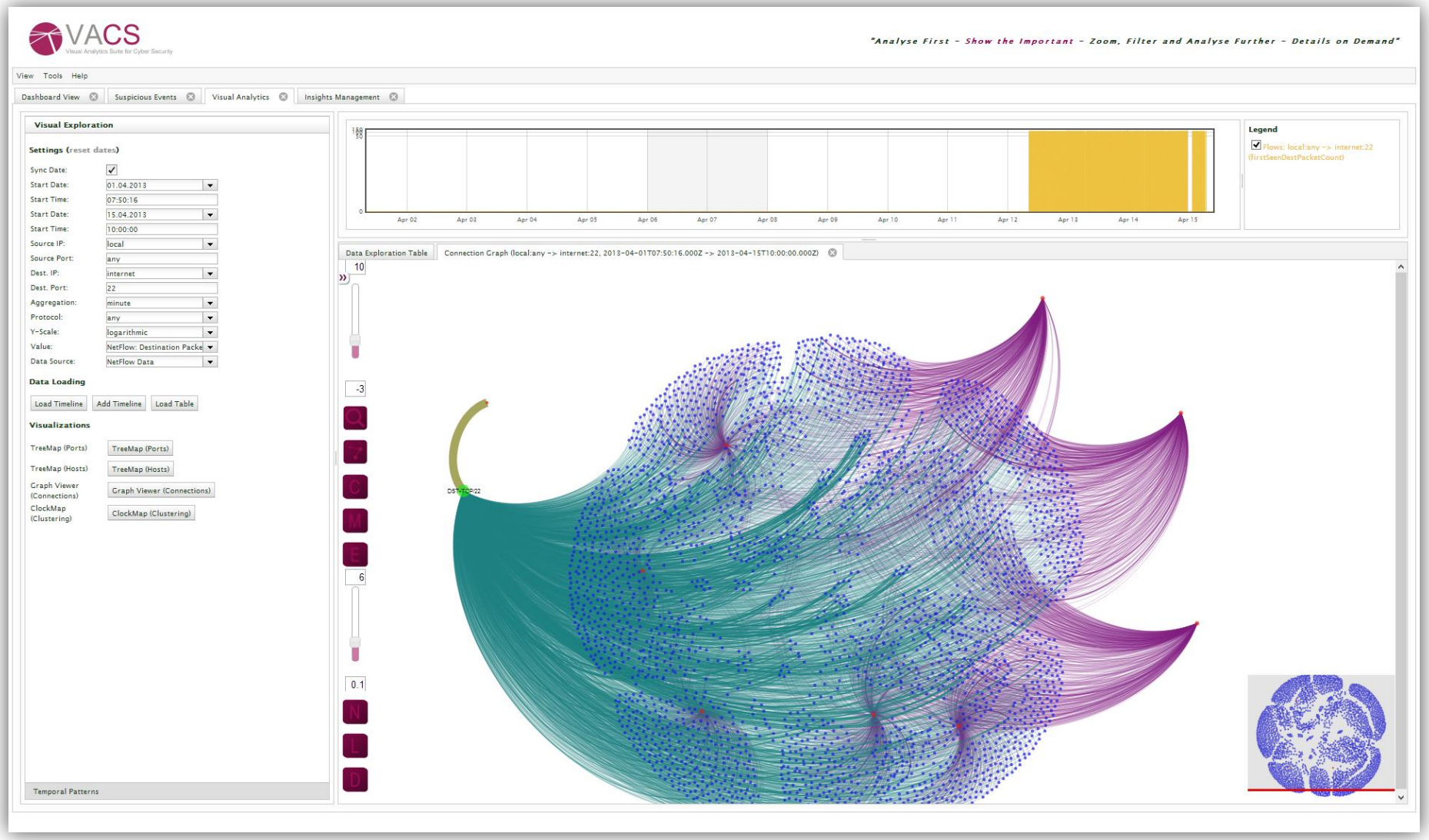
Port TreeMap for Temporal Selection



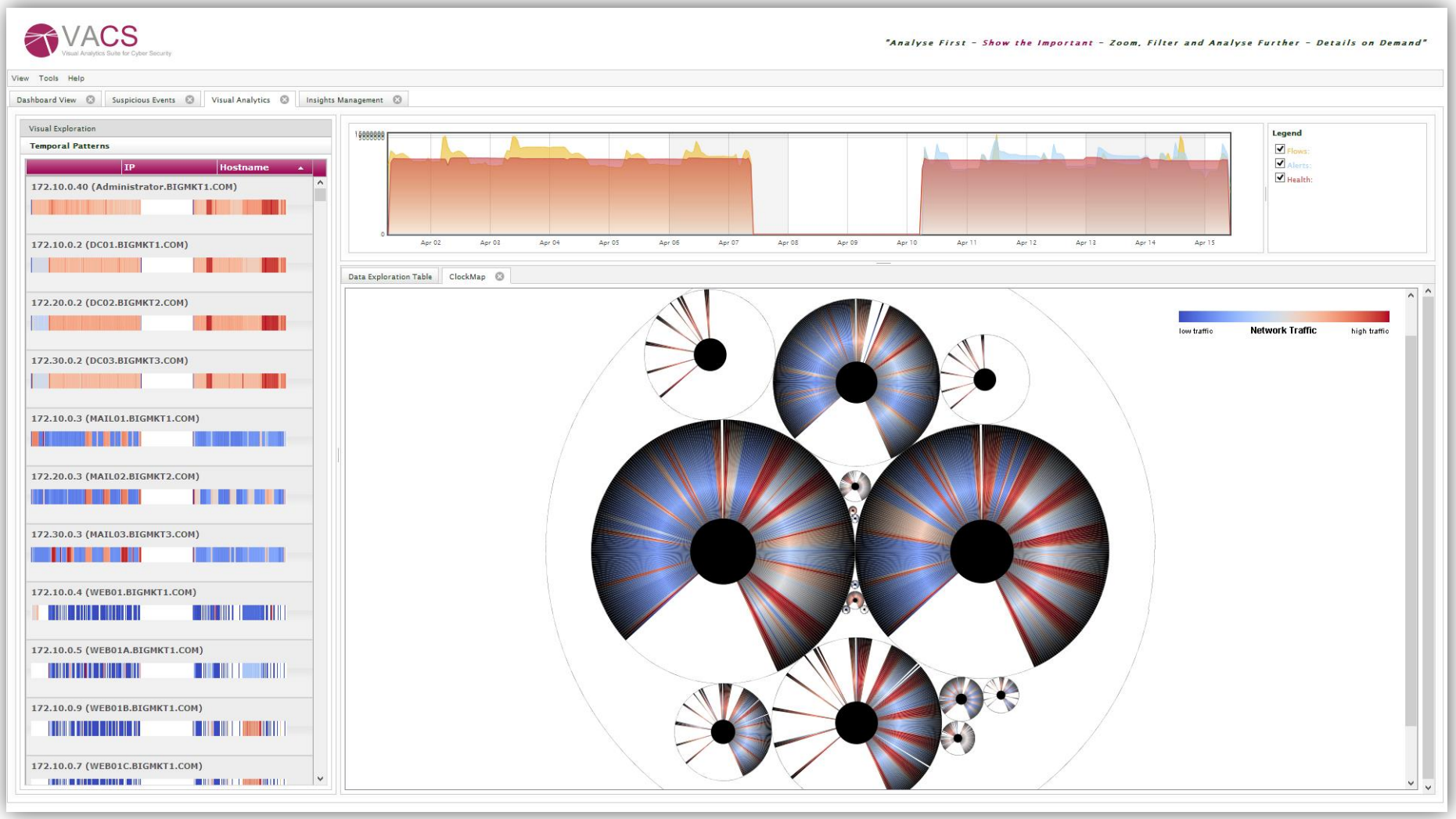
IP TreeMap for Temporal Selection



Graph Viewer for Network Connections



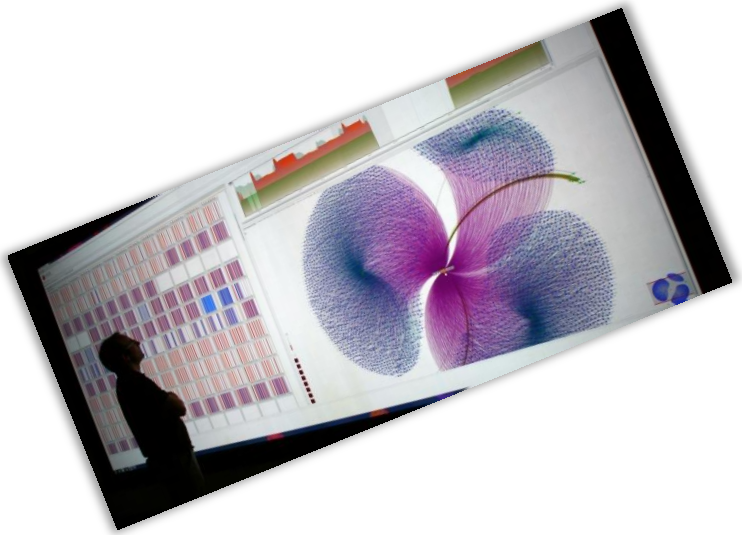
Hierarchical ClockMap



Conclusions

- **Web-Based Visual Exploration Suite (VACS)**
  - Integration of a variety of different visualizations.
- **Limitations**
  - General approach not specific for VAST Challenge.
  - Not all challenge data incorporated.
- **Future Work**
  - Glyph-based representation for heterogeneous data.
  - Improve analytics to guide user to suspicious events.

Thank you very much for your attention!



Questions?

For more information about **VACS** please contact

Fabian Fischer
Tel. +49 7531 88-2780
Fabian.Fischer@uni-konstanz.de

http://ff.cx/

twitter
@f2cx

VIS-SENSE
www.vis-sense.eu

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257495.