# Multi-aspect visual analytics on largescale high-dimensional cyber security data

Victor Y Chen, Ahmad M Razip, Sungahn Ko,
Cheryl Z Qian and David S Ebert

Yujun Zeng

CISC850
Cyber Analytics

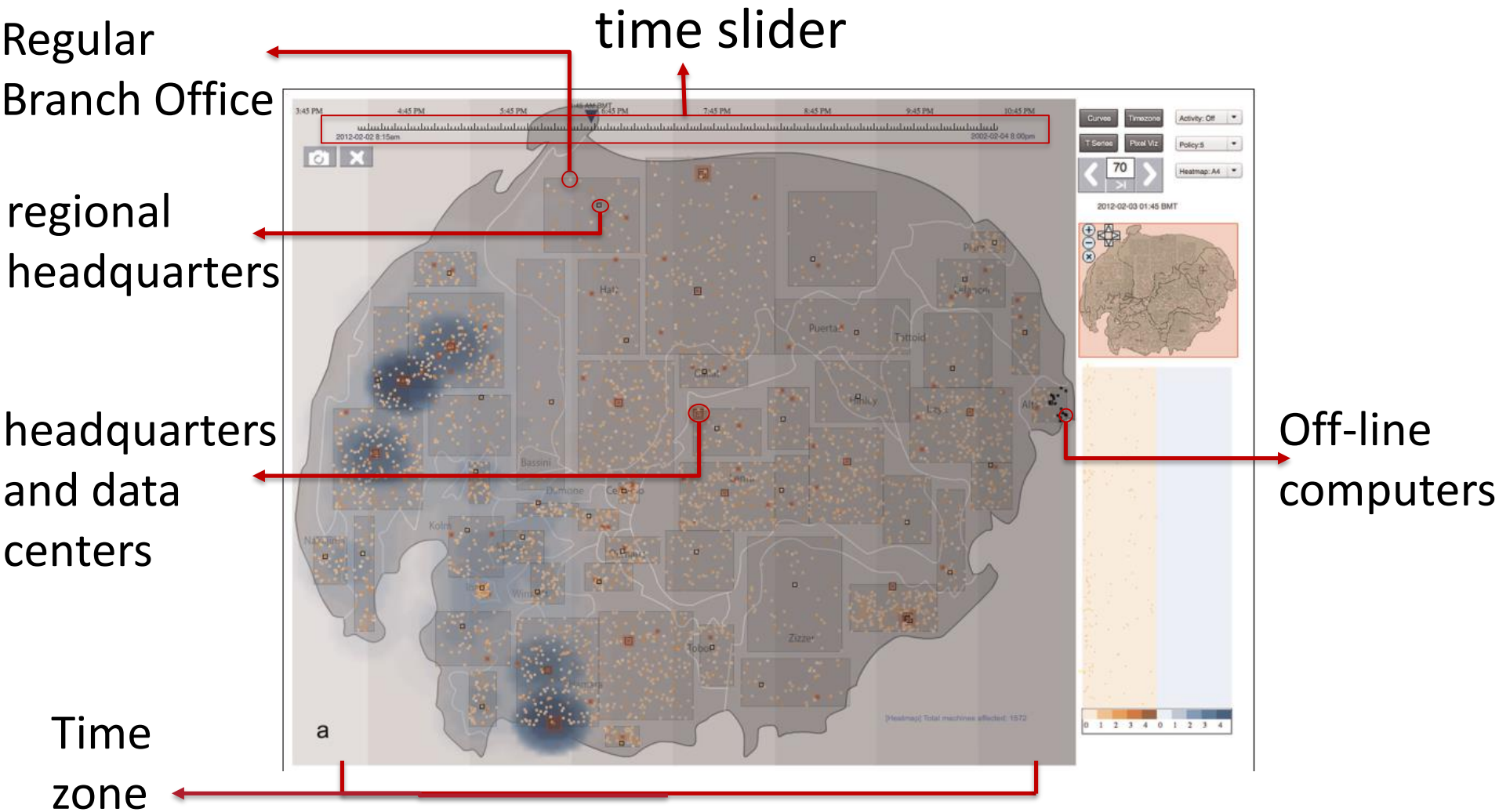
# Overview

- Introduce  SemanticPrism
- The application of SemanticPrism

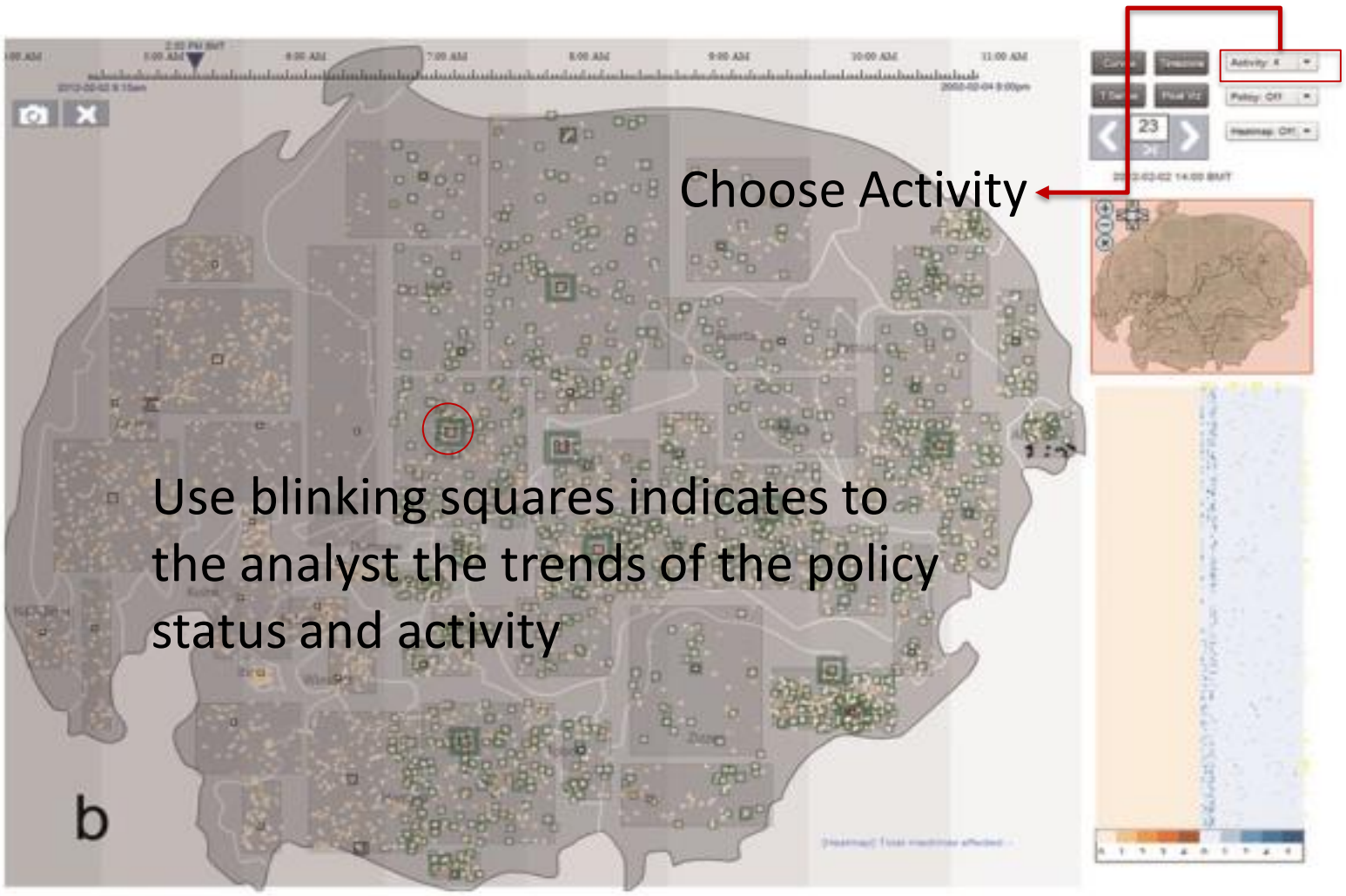
# SemanticPrism

- Aims to analyze large-scale high dimensional cyber security datasets
- Three different perspectives:
  - Spatiotemporal distribution
  - Overall temporal trends
  - Pixel-based IP address blocks

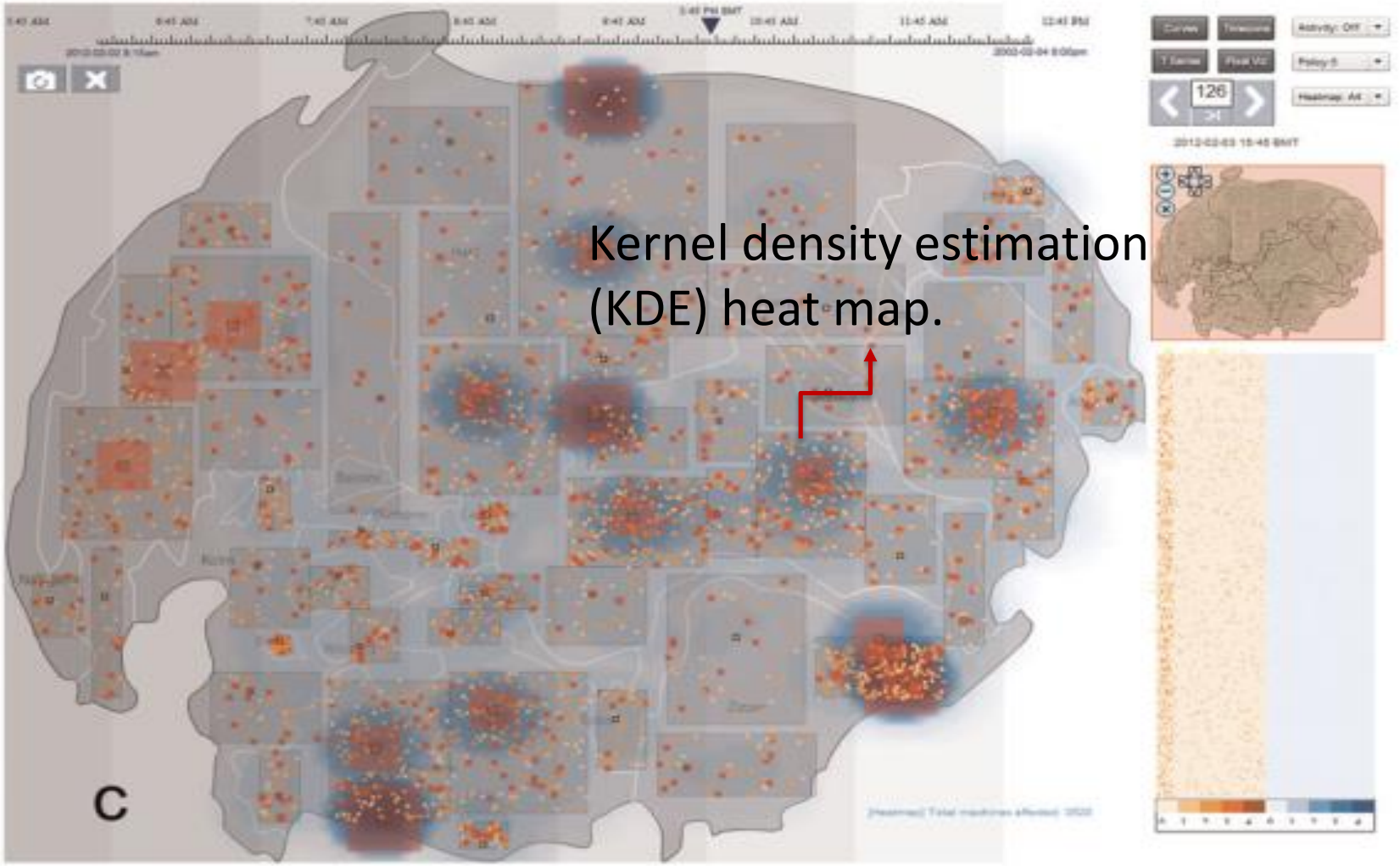
# Geospatial-temporal visualization



# Geospatial-temporal visualization



# Geospatial-temporal visualization



# Zoom and navigate

Level1:

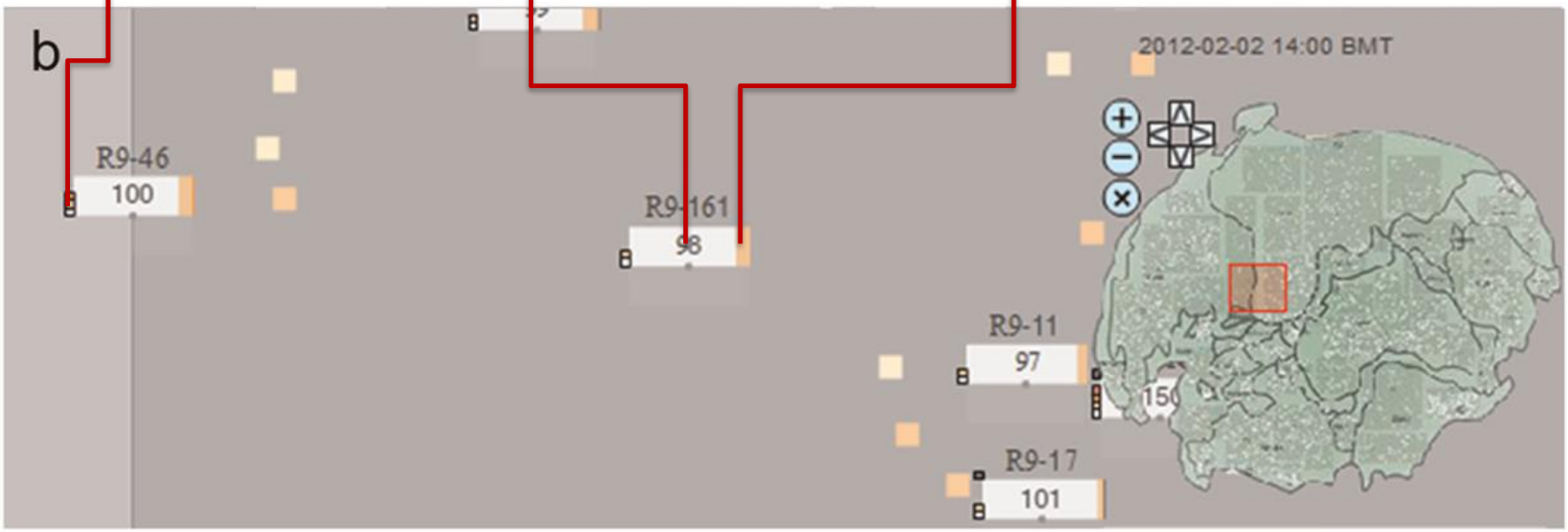
# Zoom and navigate

Level2:

to mark if computers with certain policy statuses exist

total number of computers in the office

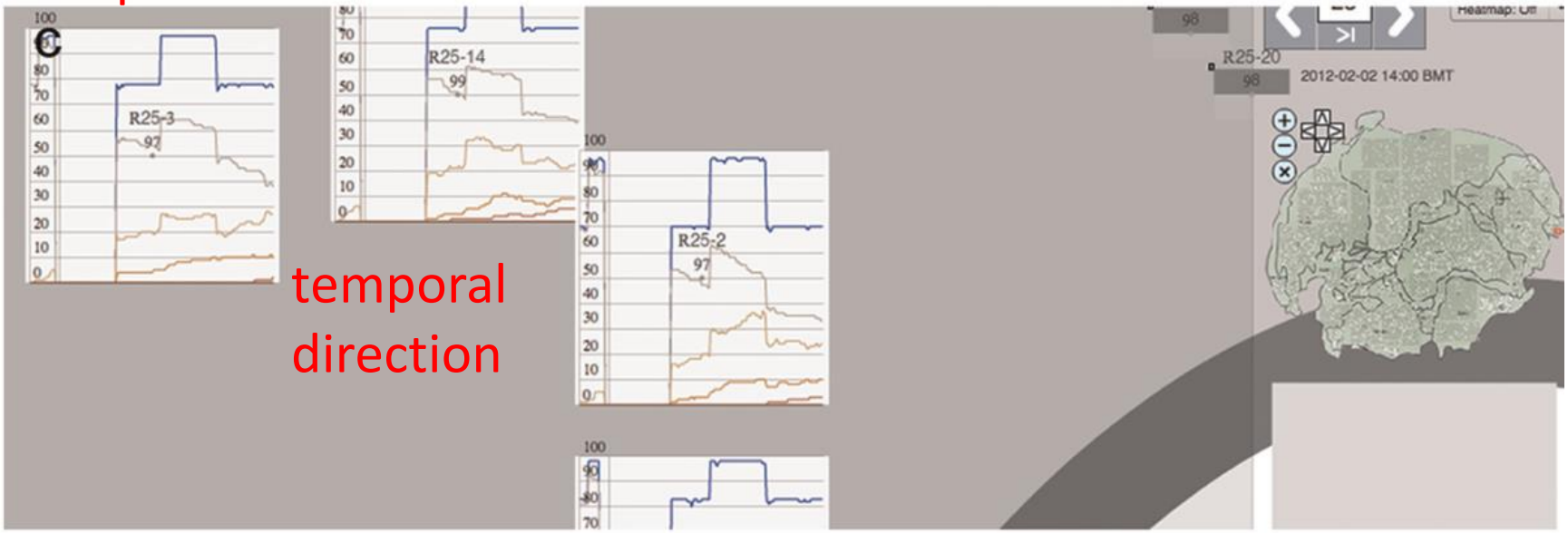
the percentage of computers with different policy statuses



# Zoom and navigate

Level3:

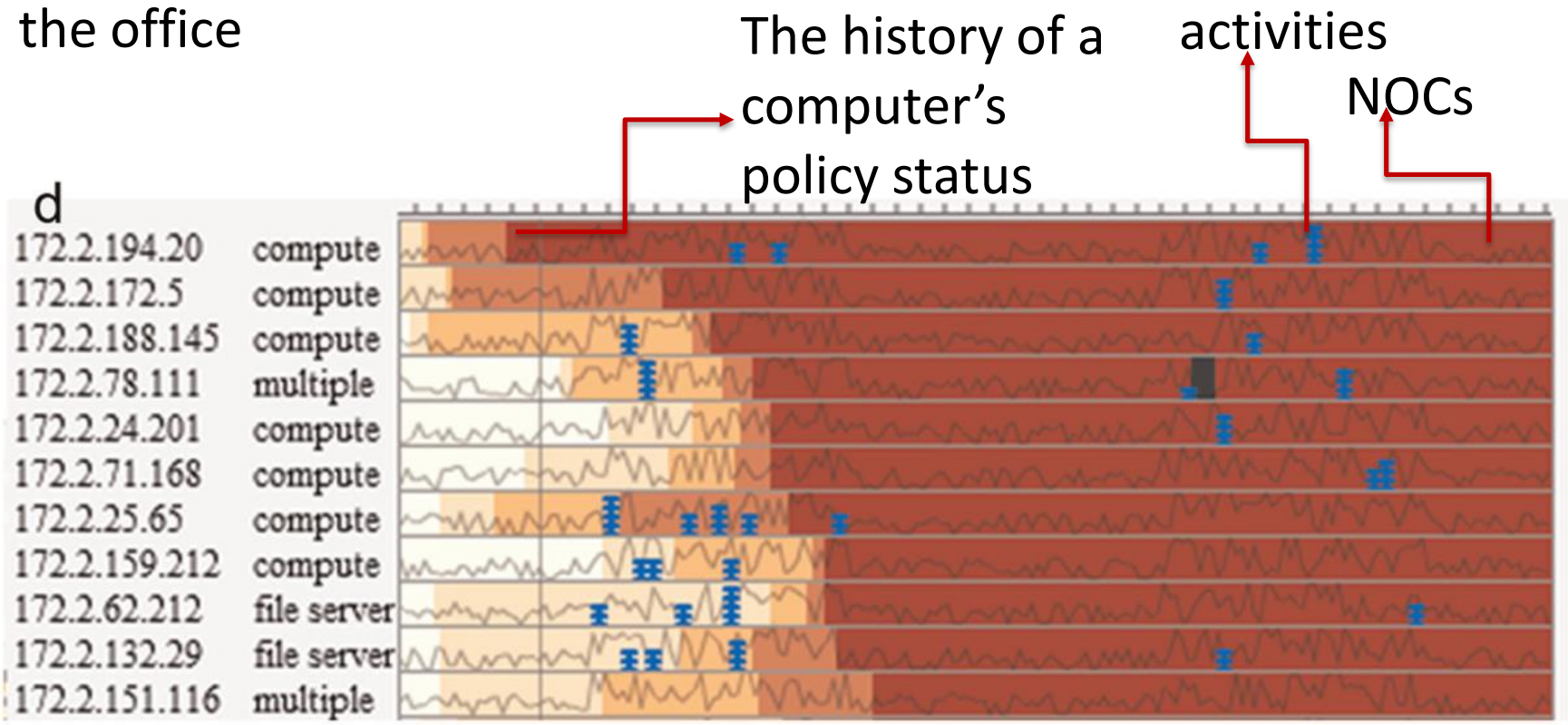
number of computers



# Zoom and navigate

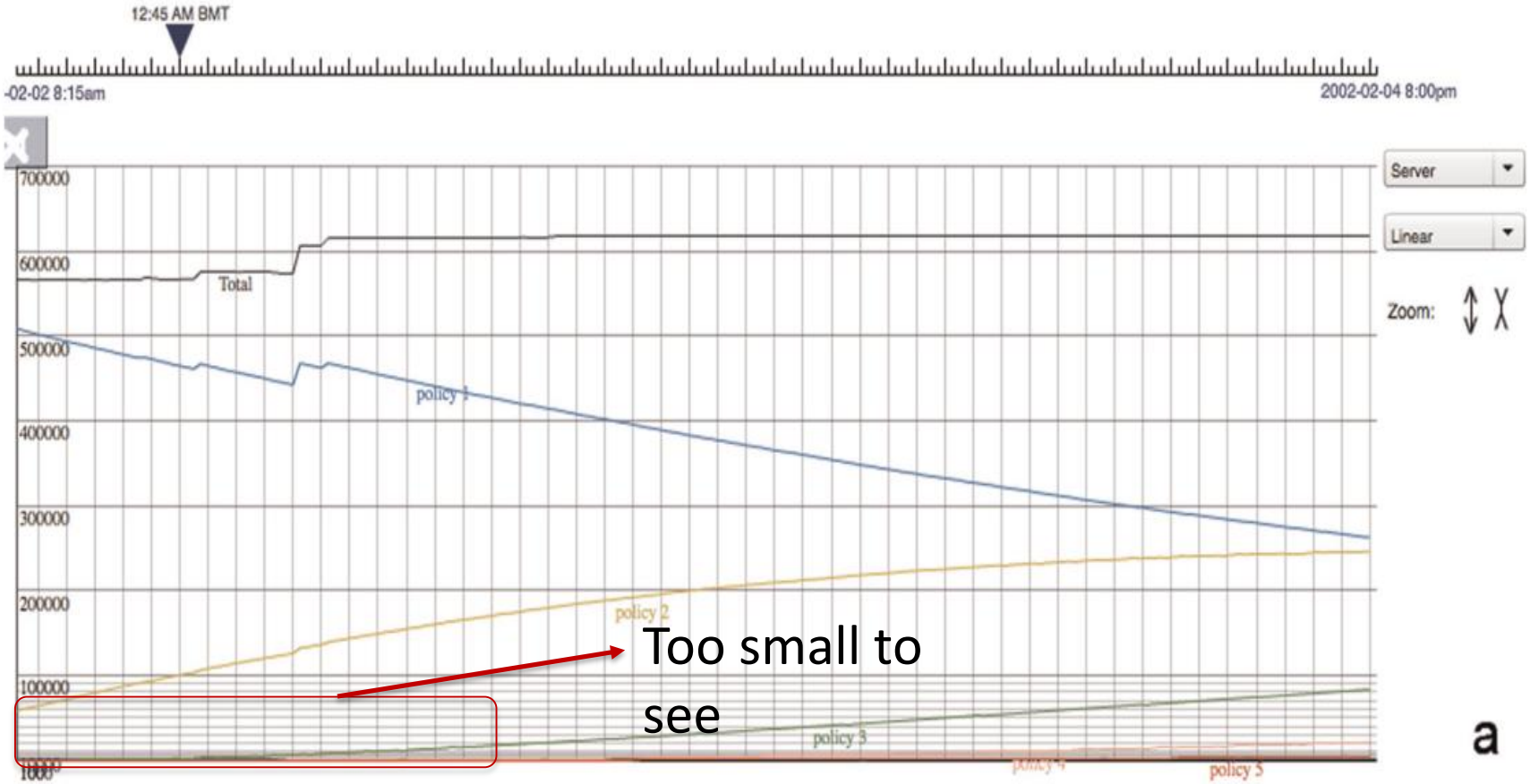
Level4:

history status of each individual computer within the office



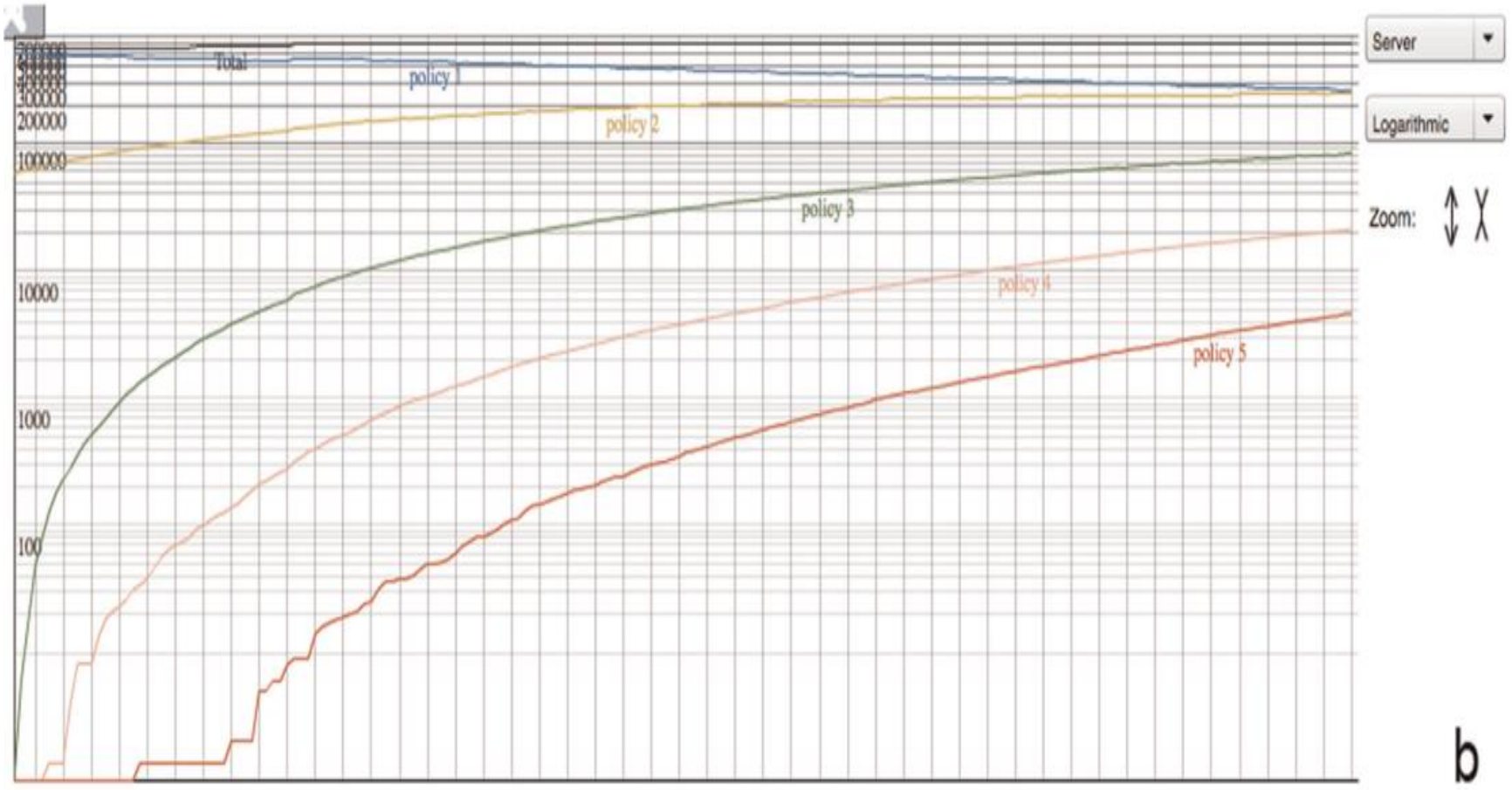
# Time series curves

The linear



# Time series curves

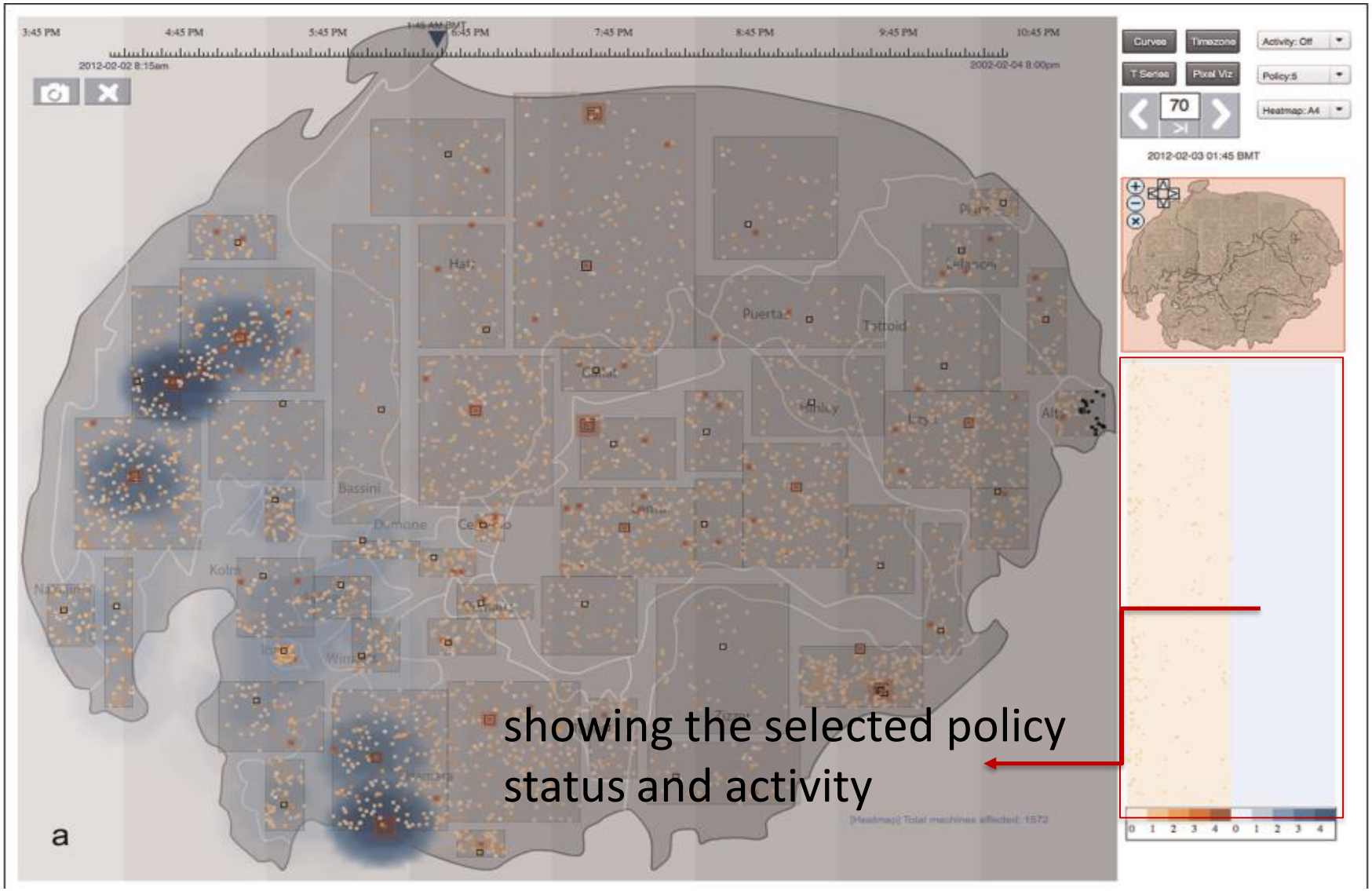
The logarithmic



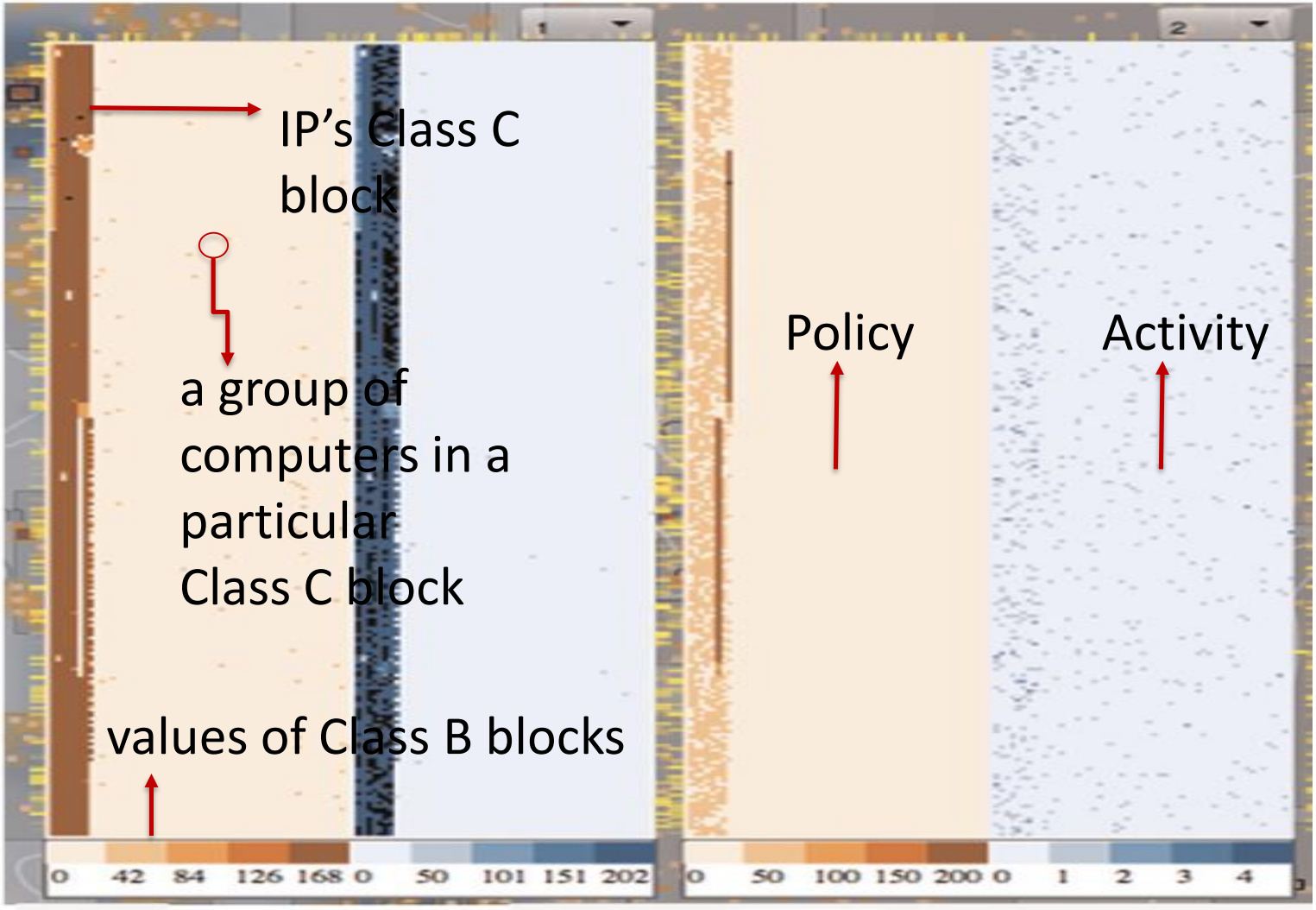
# Time series curves

# Time series curves

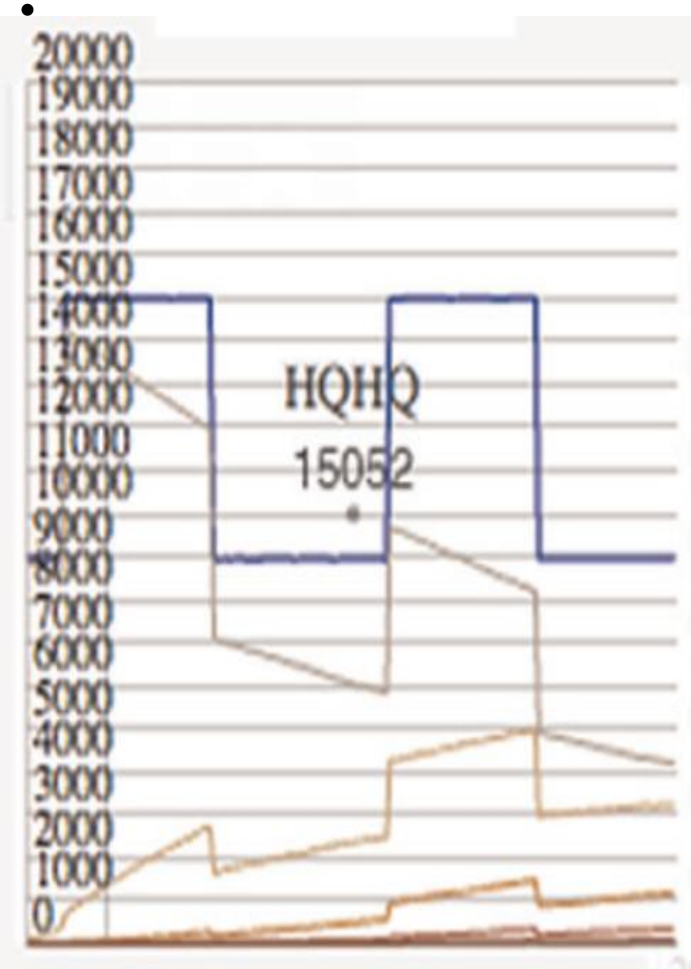
# Pixel-based visualizations

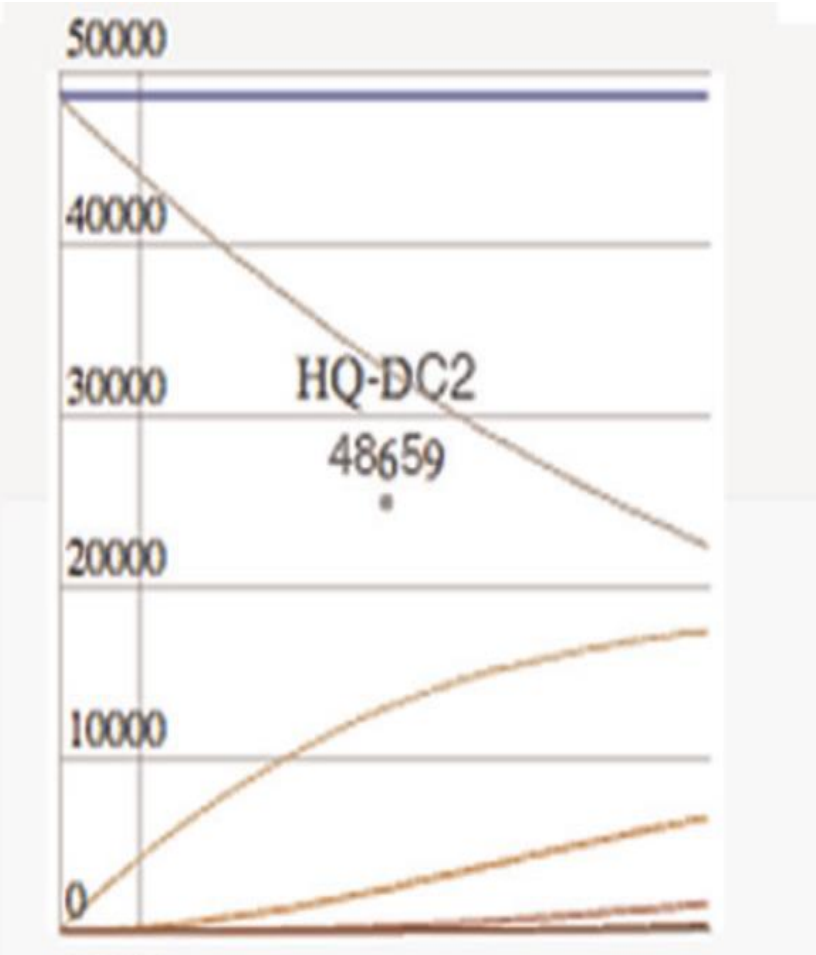


# Pixel-based visualizations



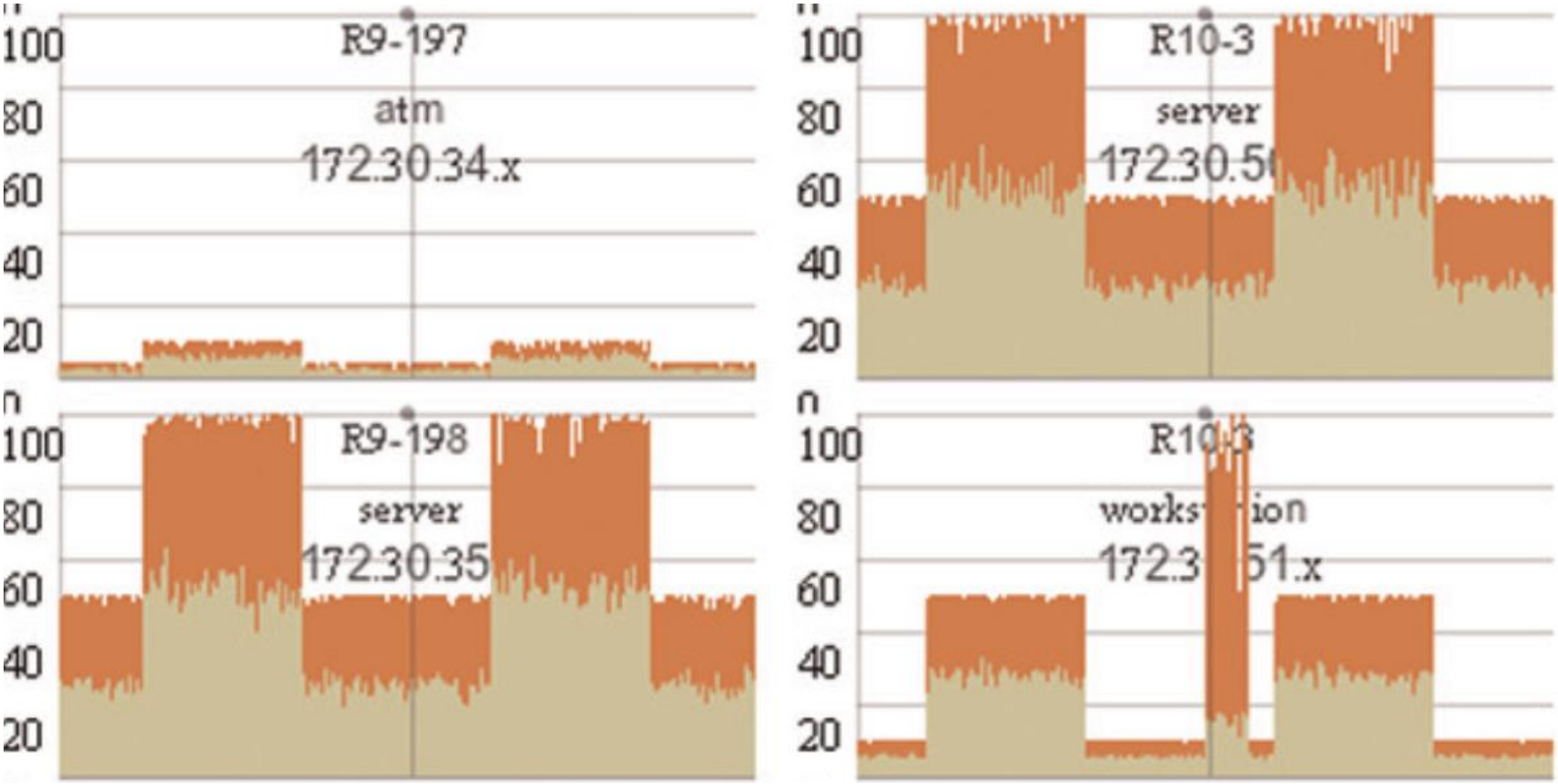
# Pixel-based visualizations



# Pixel-based visualizations

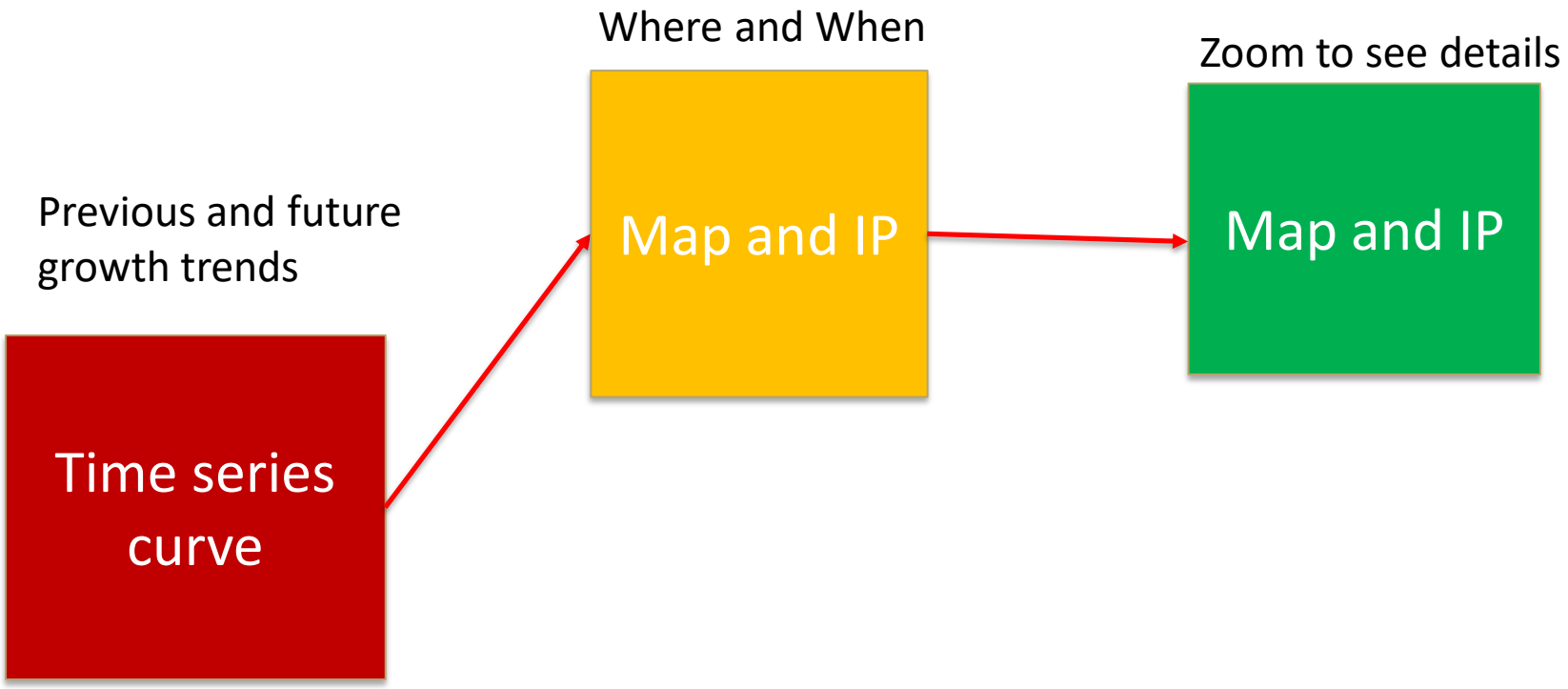
- The user can choose to see the curves of NOCs statuses



# The application of SemanticPrism

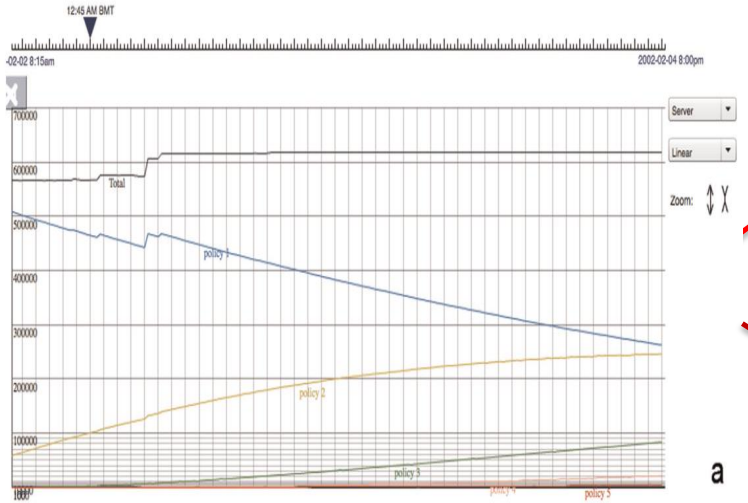
- Detection of problematic computers at an early stage
- Overall trend of policy violations and activities

# Detection of problematic computers at an early stage



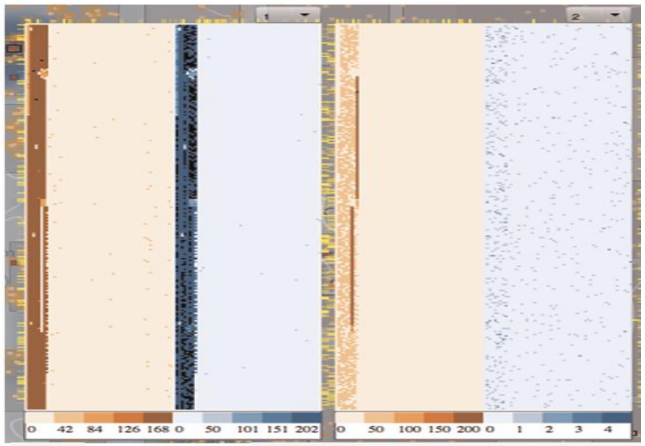
# Overall trend of policy violations and activities

Know there is a growth




Know the spatial pattern of the spread


And




see that more and more IP blocks are affected

# Thank You!