Universität
Konstanz

The National Archives (UK), 2011

BANKSAFE: A Situational Awareness Tool for Large-Scale Computer Networks

Award for Outstanding Comprehensive Submission

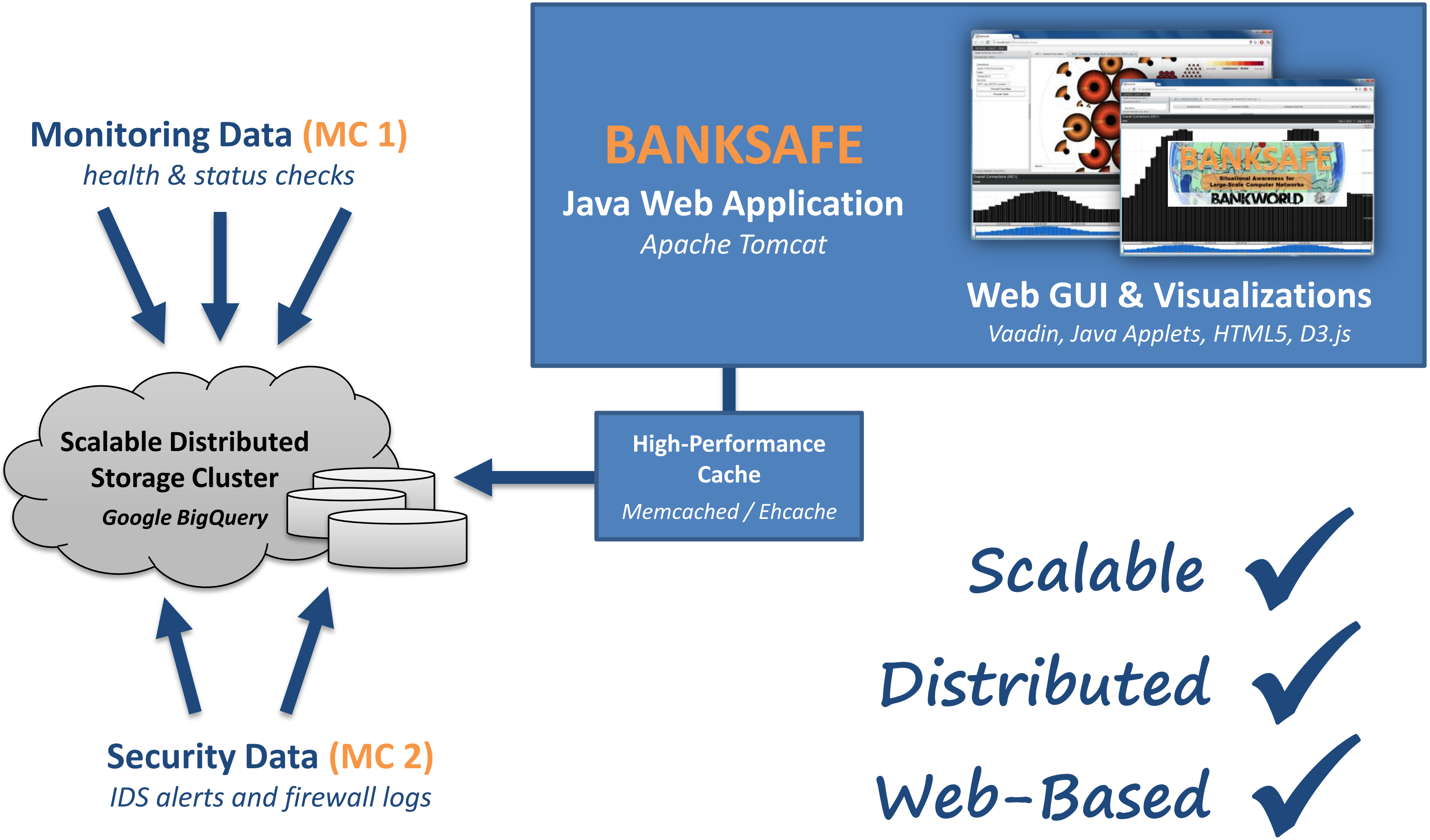
Fabian Fischer, Johannes Fuchs, Florian Mansmann, Daniel A. Keim

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.

BANKSAFE – Introduction



Monitoring Data (MC 1)
health & status checks

Scalable Distributed Storage Cluster
Google BigQuery

Security Data (MC 2)
IDS alerts and firewall logs

BANKSAFE
Java Web Application
Apache Tomcat

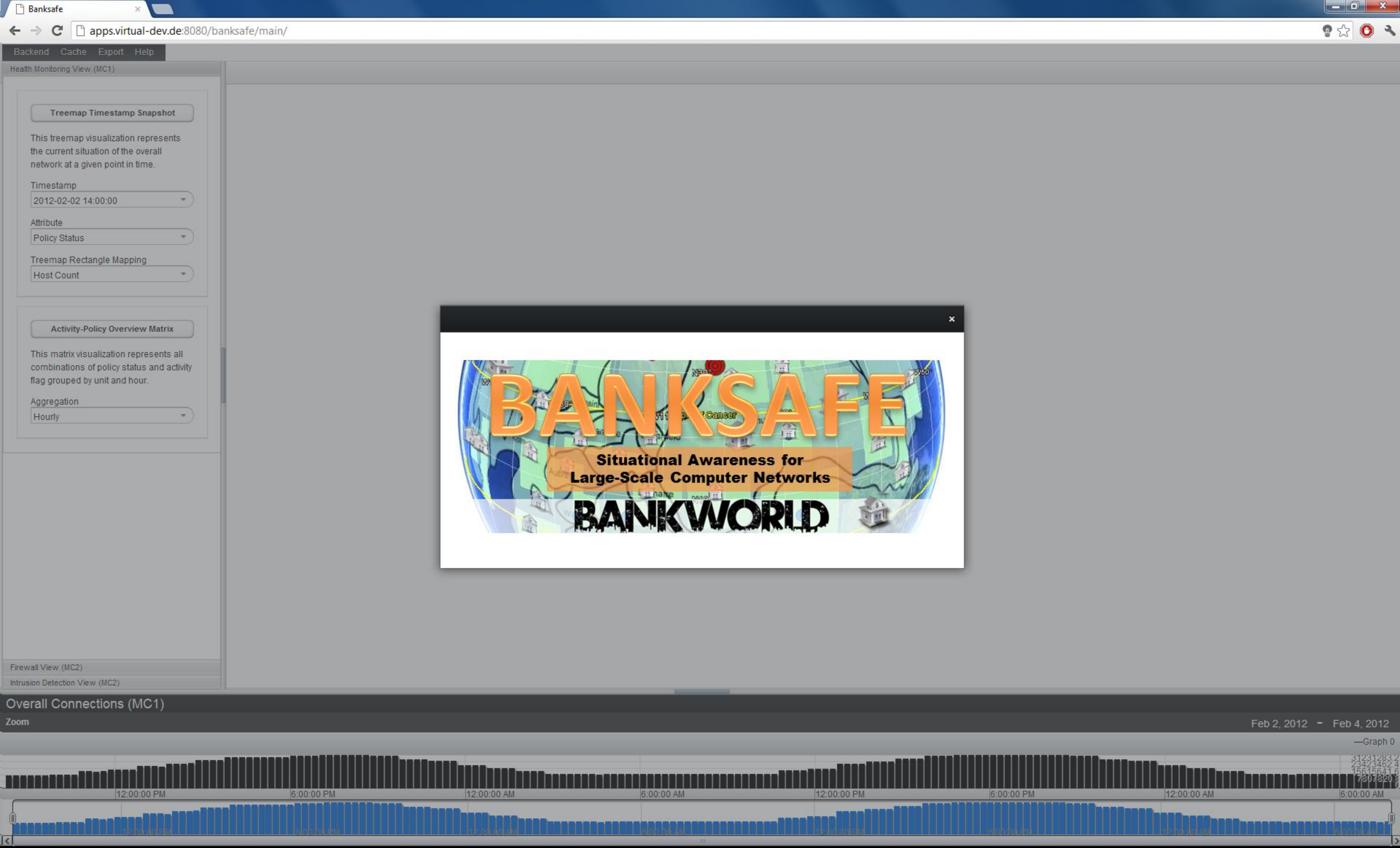
Web GUI & Visualizations
Vaadin, Java Applets, HTML5, D3.js

High-Performance Cache
Memcached / Ehcache

Scalable ✓

Distributed ✓

Web-Based ✓



Health Monitoring View (MC1)

Treemap Timestamp Snapshot

This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

Attribute: Policy Status

Treemap Rectangle Mapping: Host Count

Activity-Policy Overview Matrix

This matrix visualization represents all combinations of policy status and activity flag grouped by unit and hour.

Aggregation: Hourly

Firewall View (MC2)

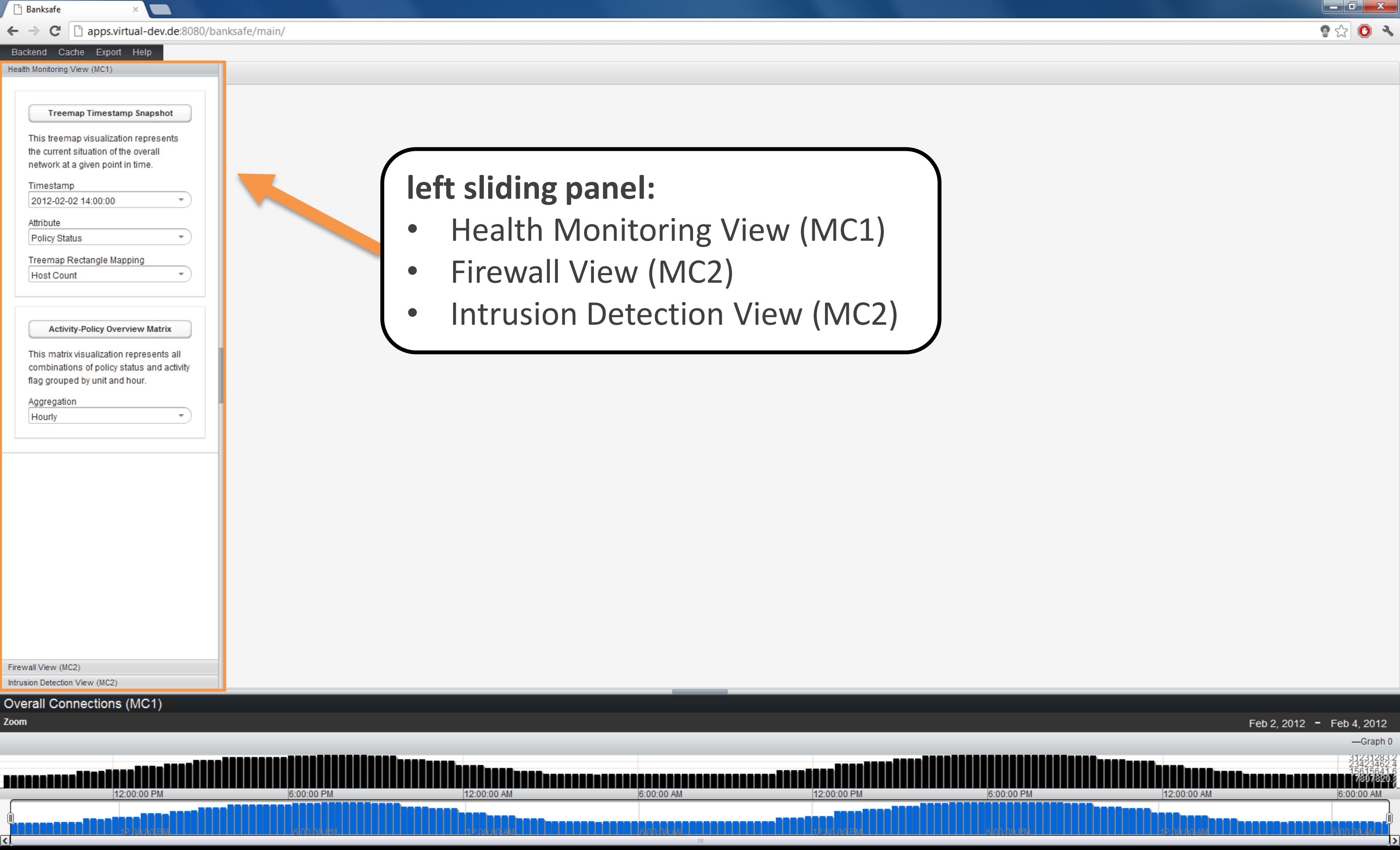
Intrusion Detection View (MC2)

BANKSAFE

Situational Awareness for Large-Scale Computer Networks

BANKWORLD

Overall Connections (MC1)


Banksafe
apps.virtual-dev.de:8080/banksafe/main/
Backend
Cache
Export
Help
Health Monitoring View (MC1)
Treemap Timestamp Snapshot
Activity-Policy Overview Matrix
Firewall View (MC2)
Intrusion Detection View (MC2)
Overall Connections (MC1)
Zoom
Feb 2, 2012 - Feb 4, 2012
—Graph 0
12:00:00 PM
6:00:00 PM
12:00:00 AM
6:00:00 AM
12:00:00 PM
6:00:00 PM
12:00:00 AM
6:00:00 AM

This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

Attribute: Policy Status

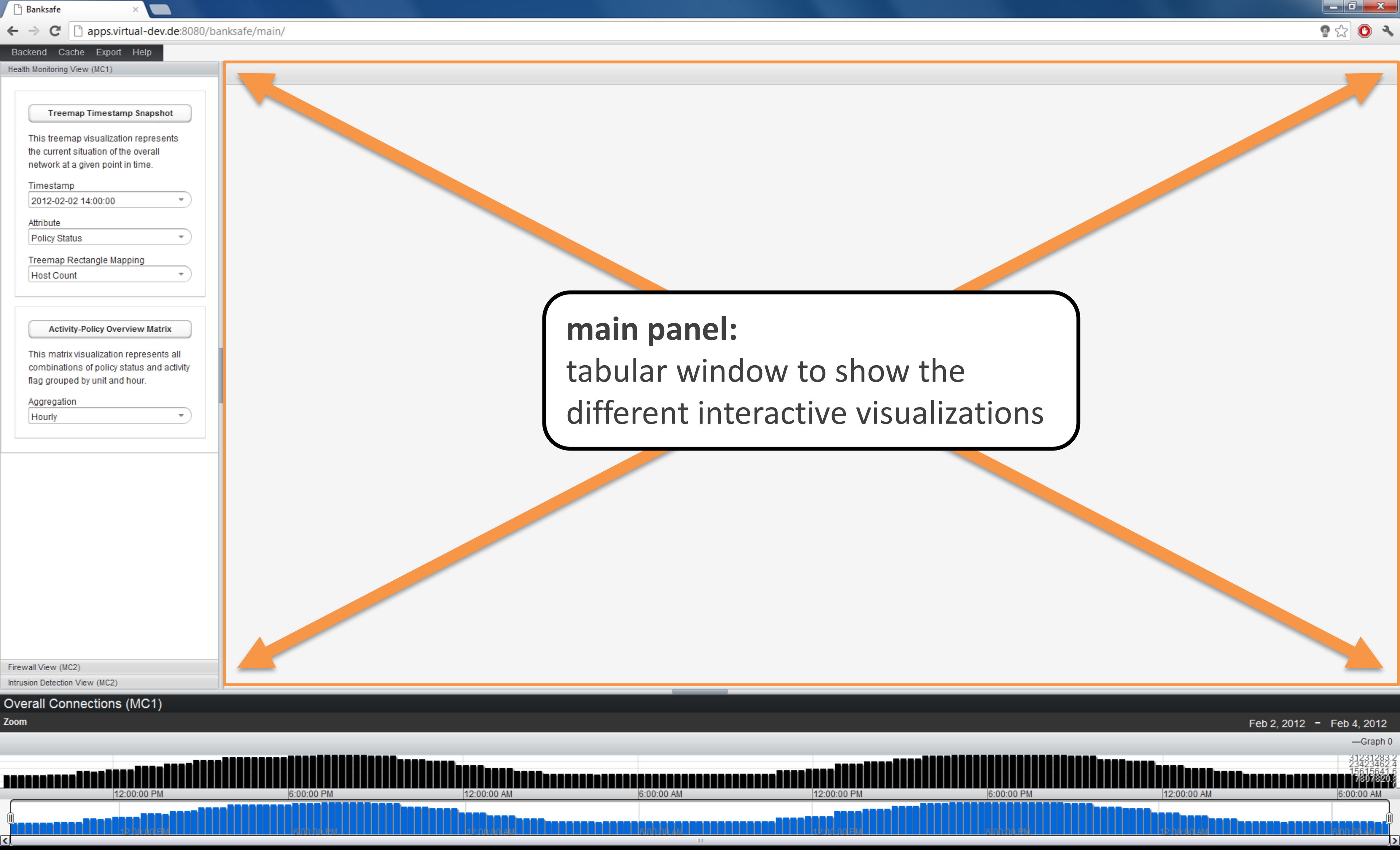
Treemap Rectangle Mapping: Host Count

This matrix visualization represents all combinations of policy status and activity flag grouped by unit and hour.

Aggregation: Hourly

left sliding panel:

- Health Monitoring View (MC1)
- Firewall View (MC2)
- Intrusion Detection View (MC2)


Banksafe
apps.virtual-dev.de:8080/banksafe/main/
Backend
Cache
Export
Help
Health Monitoring View (MC1)
Treemap Timestamp Snapshot
Activity-Policy Overview Matrix
Firewall View (MC2)
Intrusion Detection View (MC2)
Overall Connections (MC1)
Zoom
Feb 2, 2012 - Feb 4, 2012
—Graph 0
12:00:00 PM
6:00:00 PM
12:00:00 AM
6:00:00 AM
12:00:00 PM
6:00:00 PM
12:00:00 AM
6:00:00 AM

This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

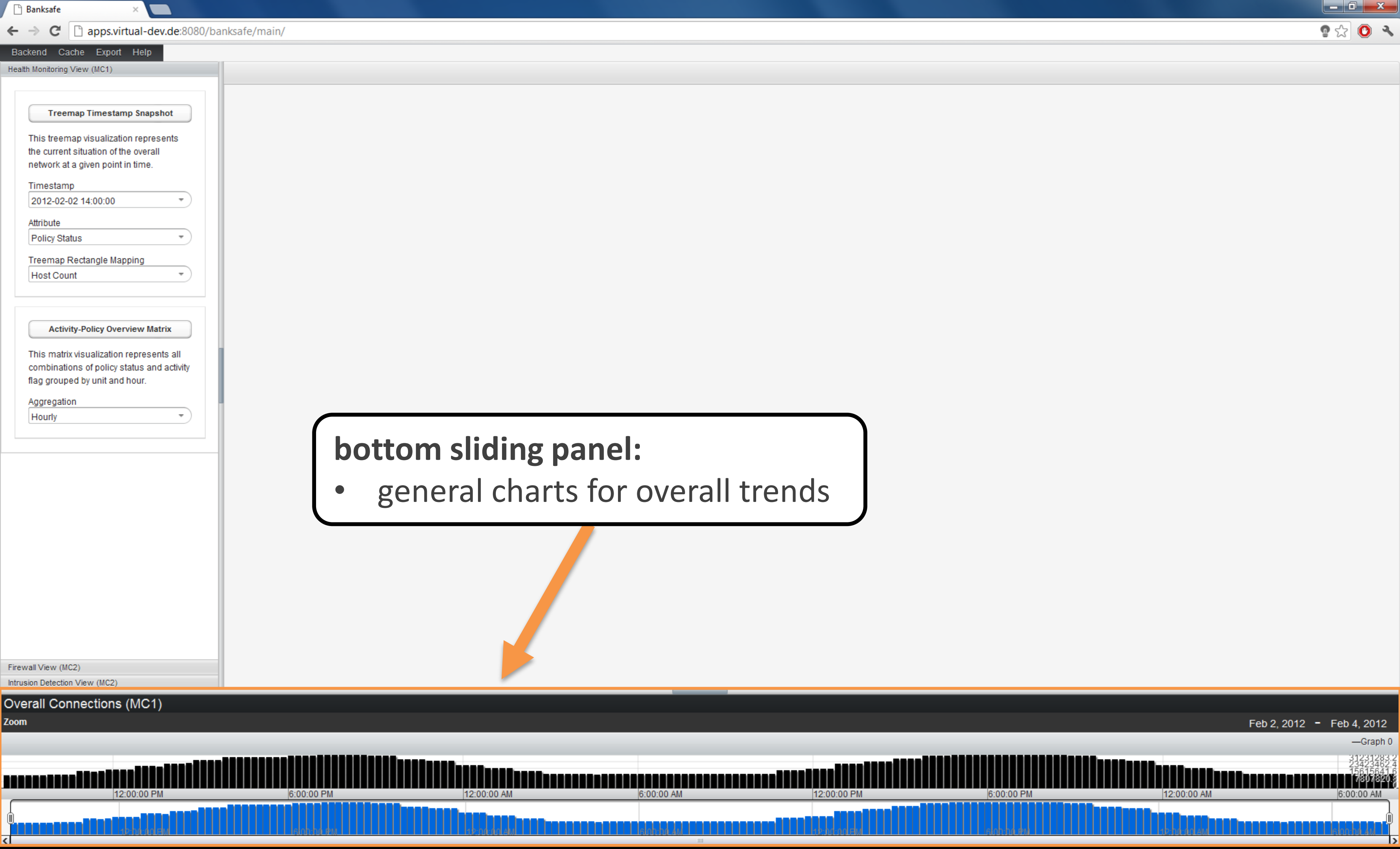
Attribute: Policy Status

Treemap Rectangle Mapping: Host Count

This matrix visualization represents all combinations of policy status and activity flag grouped by unit and hour.

Aggregation: Hourly

main panel:
tabular window to show the different interactive visualizations



Banksafe
apps.virtual-dev.de:8080/banksafe/main/
Backend
Cache
Export
Help
Health Monitoring View (MC1)
Treemap Timestamp Snapshot
Activity-Policy Overview Matrix
Firewall View (MC2)
Intrusion Detection View (MC2)
Overall Connections (MC1)
Zoom
Feb 2, 2012 - Feb 4, 2012
—Graph 0
12:00:00 PM
6:00:00 PM
12:00:00 AM
6:00:00 AM
12:00:00 PM
6:00:00 PM
12:00:00 AM
6:00:00 AM

This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

Attribute: Policy Status

Treemap Rectangle Mapping: Host Count

This matrix visualization represents all combinations of policy status and activity flag grouped by unit and hour.

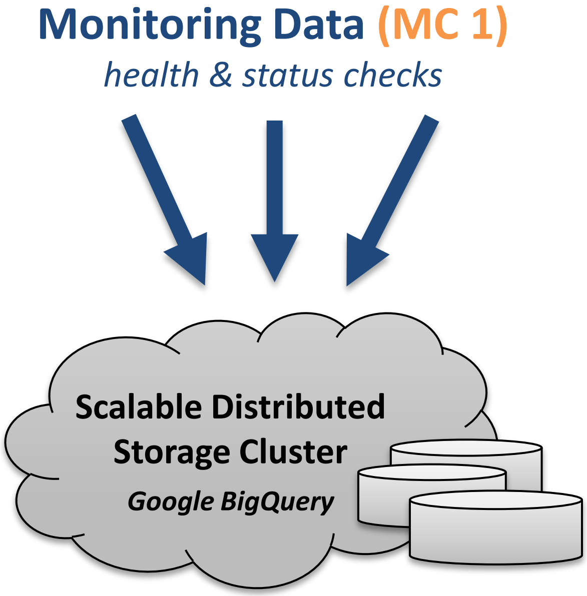
Aggregation: Hourly

bottom sliding panel:

- general charts for overall trends

Network Health Monitoring (MC 1)

Mini Challenge 1



Monitoring Data (MC 1)

health & status checks

Scalable Distributed Storage Cluster

Google BigQuery

- **health and status checks**
  - status of all machines, every 15 minutes
    - e.g., **policy level**, **activity flag**

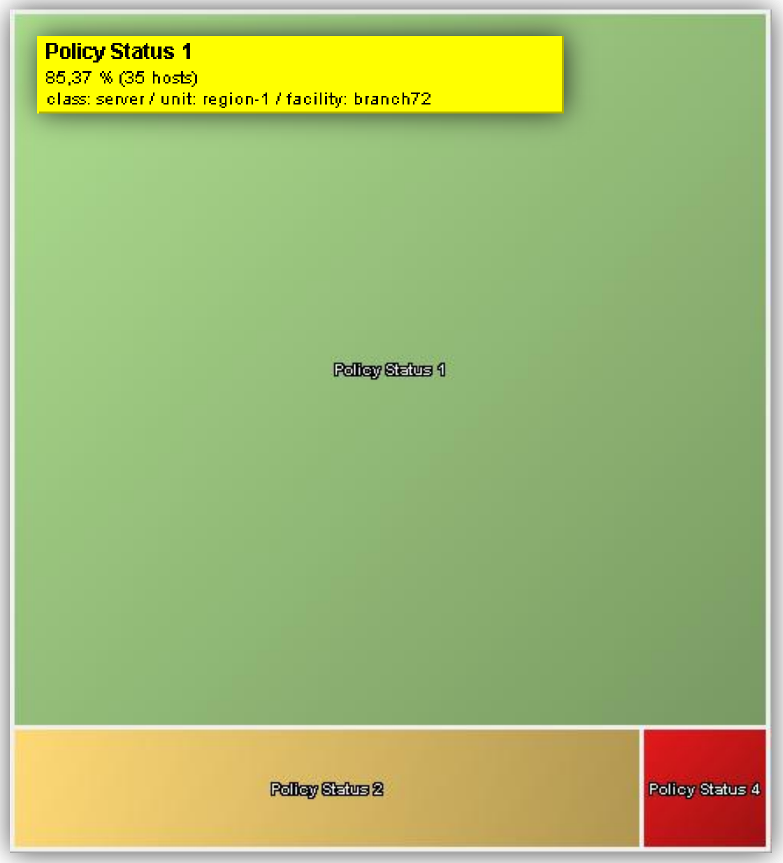
policy	meaning
1	healthy
2	moderate policy deviations
3	serious policy deviations
4	… and some patches failing
5	possible virus infection

activity	meaning
1	normal
2	maintenance
3	invalid login attempts
4	CPU fully consumed
5	external device added

Point-in-Time Health Overview

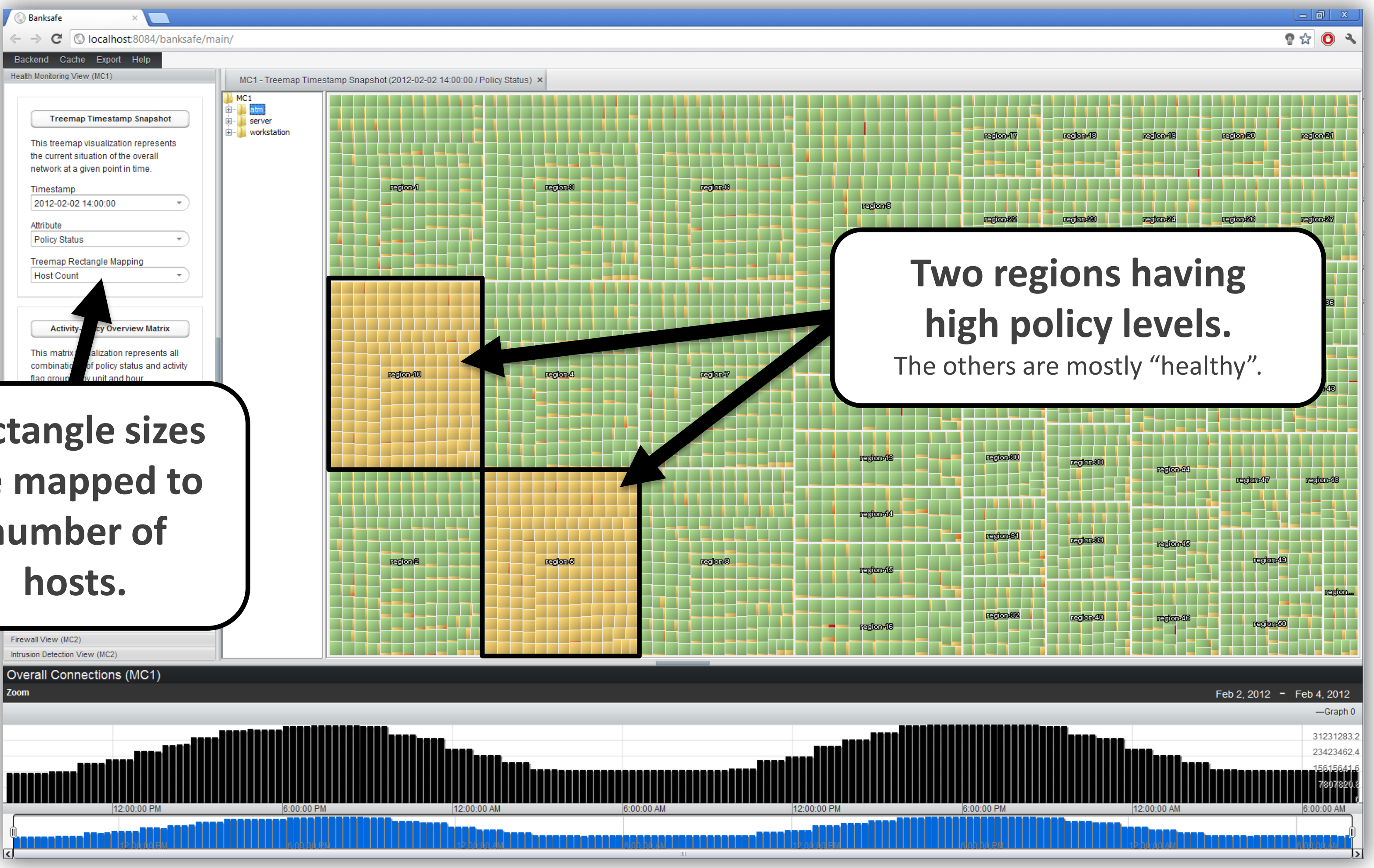
Visualizations for Health Monitoring (MC 1)

- **Treemap Visualization**
  - focusing on the percentage distribution
  - space-filling hierarchical representation
- **Example** (on the right)
  - number of servers
  - for the policy levels
  - region-1 / branch72


Policy Status 1
85,37 % (35 hosts)
class: server / unit: region-1 / facility: branch72

Point-in-Time Health Overview

Visualizations for Health Monitoring (MC 1)



Treemap Timestamp Snapshot

This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

Attribute: Policy Status

Treemap Rectangle Mapping: Host Count

Activity- cy Overview Matrix

This matrix alization represents all combinati of policy status and activity flag group y unit and hour.

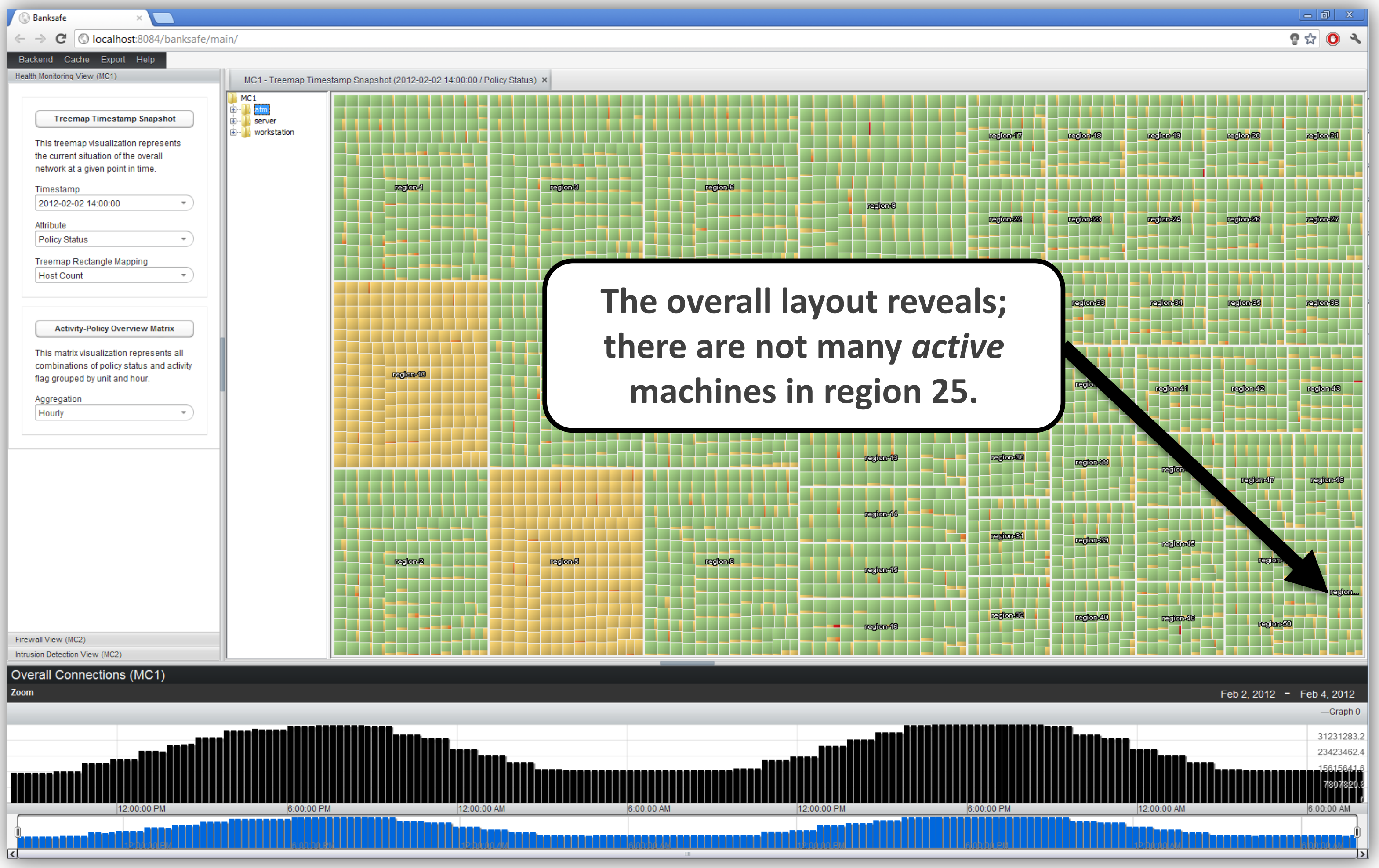
Rectangle sizes are mapped to number of hosts.

Two regions having high policy levels.

The others are mostly "healthy".

Point-in-Time Health Overview

Visualizations for Health Monitoring (MC 1)



Treemap Timestamp Snapshot

This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

Attribute: Policy Status

Treemap Rectangle Mapping: Host Count

Activity-Policy Overview Matrix

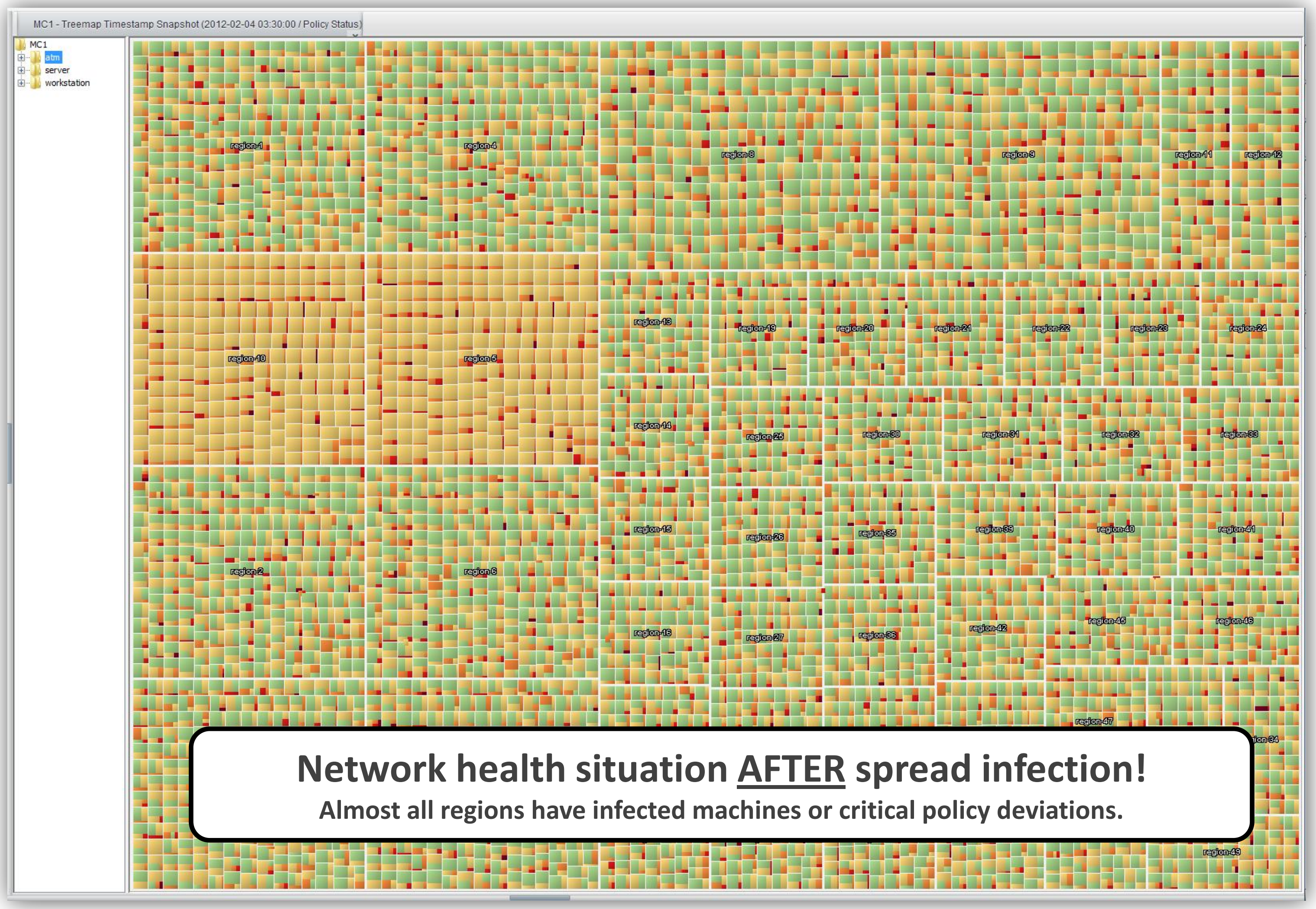
This matrix visualization represents all combinations of policy status and activity flag grouped by unit and hour.

Aggregation: Hourly

The overall layout reveals; there are not many *active* machines in region 25.

Point-in-Time Health Overview

Visualizations for Health Monitoring (MC 1)

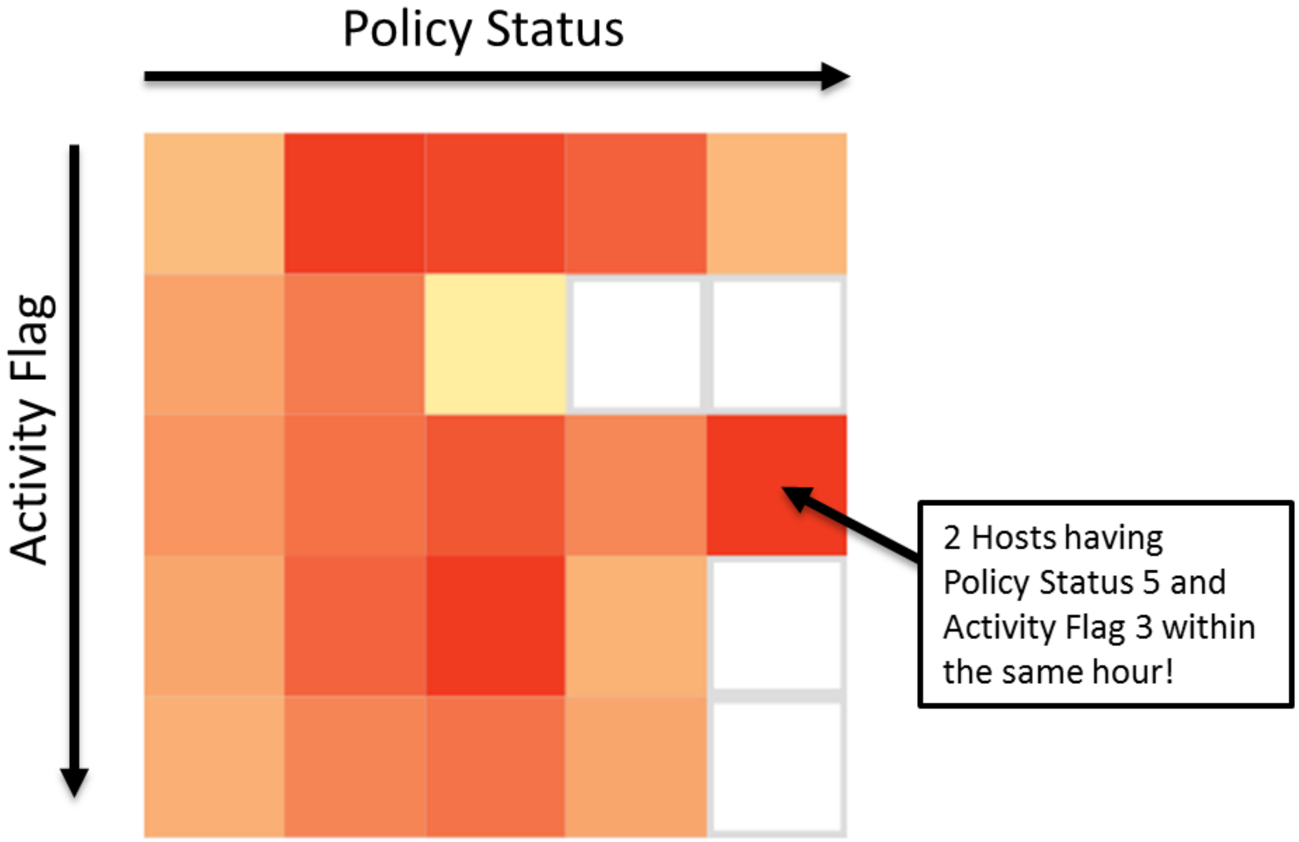


Network health situation AFTER spread infection!

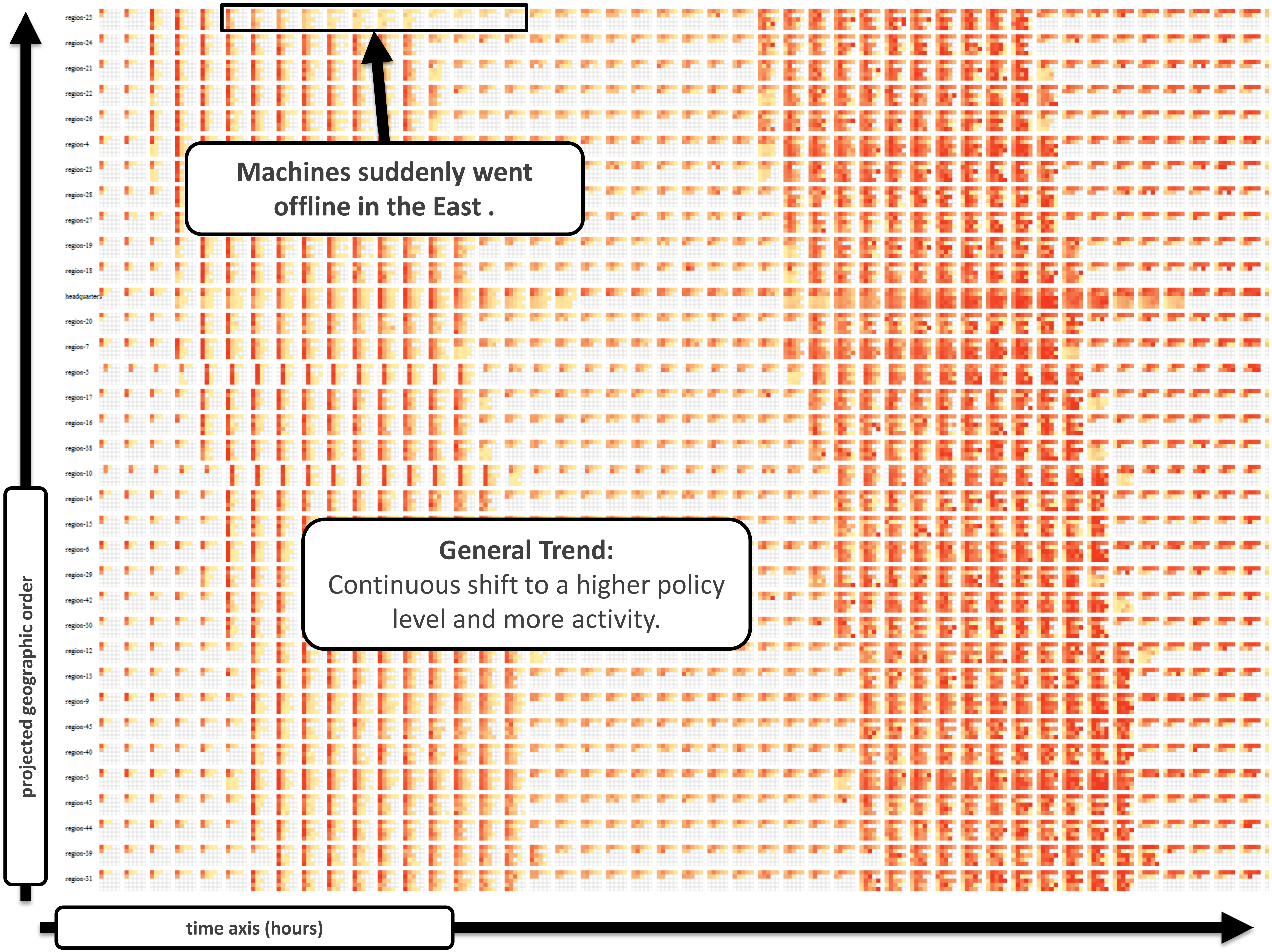
Almost all regions have infected machines or critical policy deviations.

Temporal Health Trend Overview

Visualizations for Health Monitoring (MC 1)



2 Hosts having Policy Status 5 and Activity Flag 3 within the same hour!

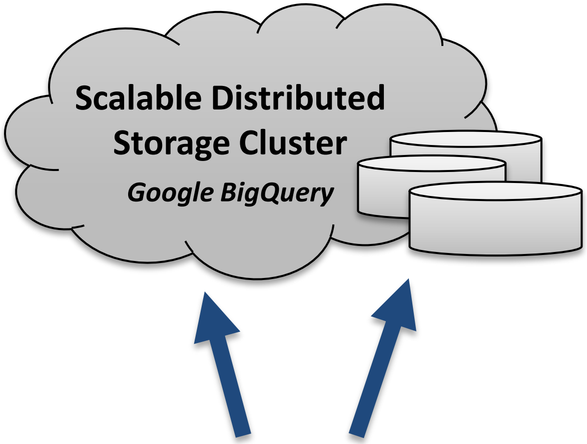


Machines suddenly went offline in the East .

General Trend:
Continuous shift to a higher policy level and more activity.

Exploration of Security Data (MC 2)

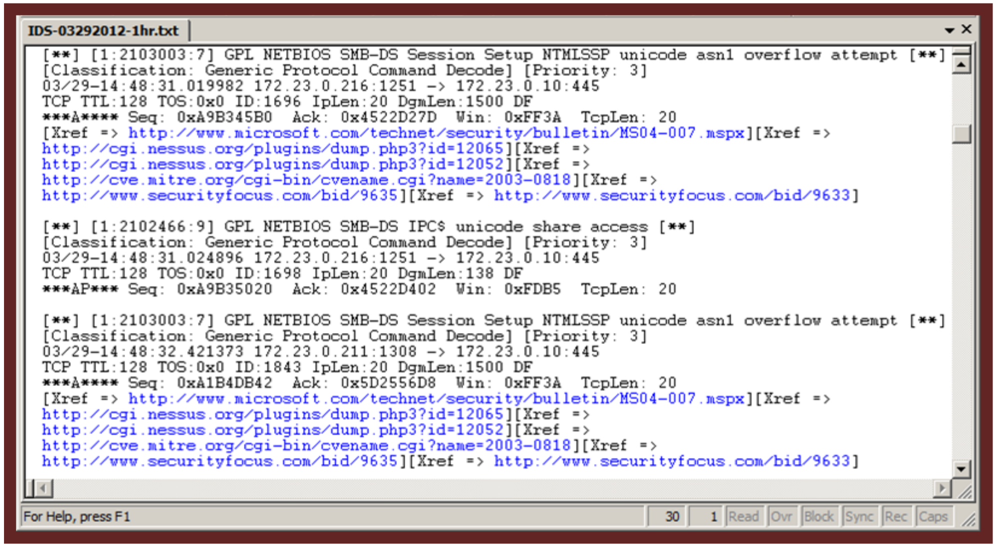
Mini Challenge 2



Security Data (MC 2)

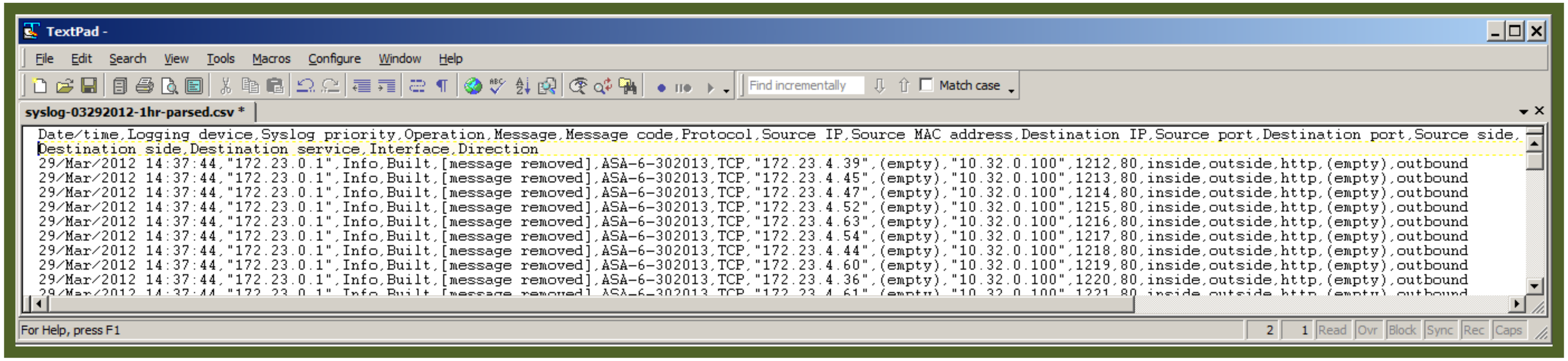
IDS alerts and firewall logs

IDS Alerts



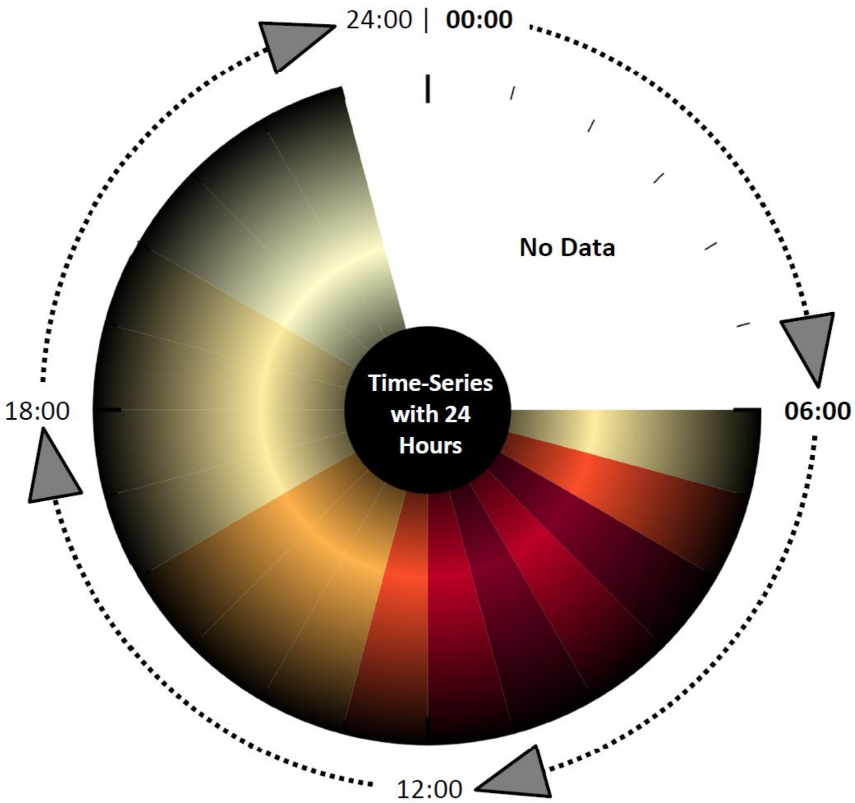
```
[**] [1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
03/29-14:48:31.019982 172.23.0.216:1251 -> 172.23.0.10:445
TCP TTL:128 TOS:0x0 ID:1696 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xA9B345B0  Ack: 0x4522D27D  Win: 0xFF3A  TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12065][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12052][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0818][Xref =>
http://www.securityfocus.com/bid/9635][Xref => http://www.securityfocus.com/bid/9633]

[**] [1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
03/29-14:48:31.024896 172.23.0.216:1251 -> 172.23.0.10:445
TCP TTL:128 TOS:0x0 ID:1698 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0xA9B35020  Ack: 0x4522D402  Win: 0xFDB5  TcpLen: 20

[**] [1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
03/29-14:48:32.421373 172.23.0.211:1308 -> 172.23.0.10:445
TCP TTL:128 TOS:0x0 ID:1843 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xA1B4DB42  Ack: 0x5D2556D8  Win: 0xFF3A  TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12065][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12052][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0818][Xref =>
http://www.securityfocus.com/bid/9635][Xref => http://www.securityfocus.com/bid/9633]
```

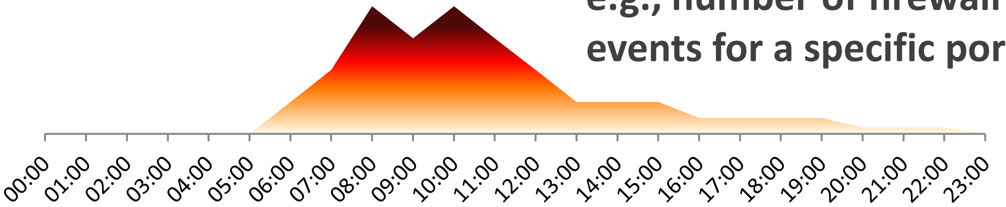
Firewall Log



```
Date/time,Logging device,Syslog priority,Operation,Message,Message code,Protocol,Source IP,Source MAC address,Destination IP,Source port,Destination port,Source side,
Destination side,Destination service,Interface,Direction
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.39",(empty),"10.32.0.100",1212,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.45",(empty),"10.32.0.100",1213,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.47",(empty),"10.32.0.100",1214,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.52",(empty),"10.32.0.100",1215,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.63",(empty),"10.32.0.100",1216,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.54",(empty),"10.32.0.100",1217,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.44",(empty),"10.32.0.100",1218,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.60",(empty),"10.32.0.100",1219,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.36",(empty),"10.32.0.100",1220,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.61",(empty),"10.32.0.100",1221,80,inside,outside,http,(empty),outbound
```

Glyph Design (Clockeye)





e.g., number of firewall events for a specific port

type = circular glyph

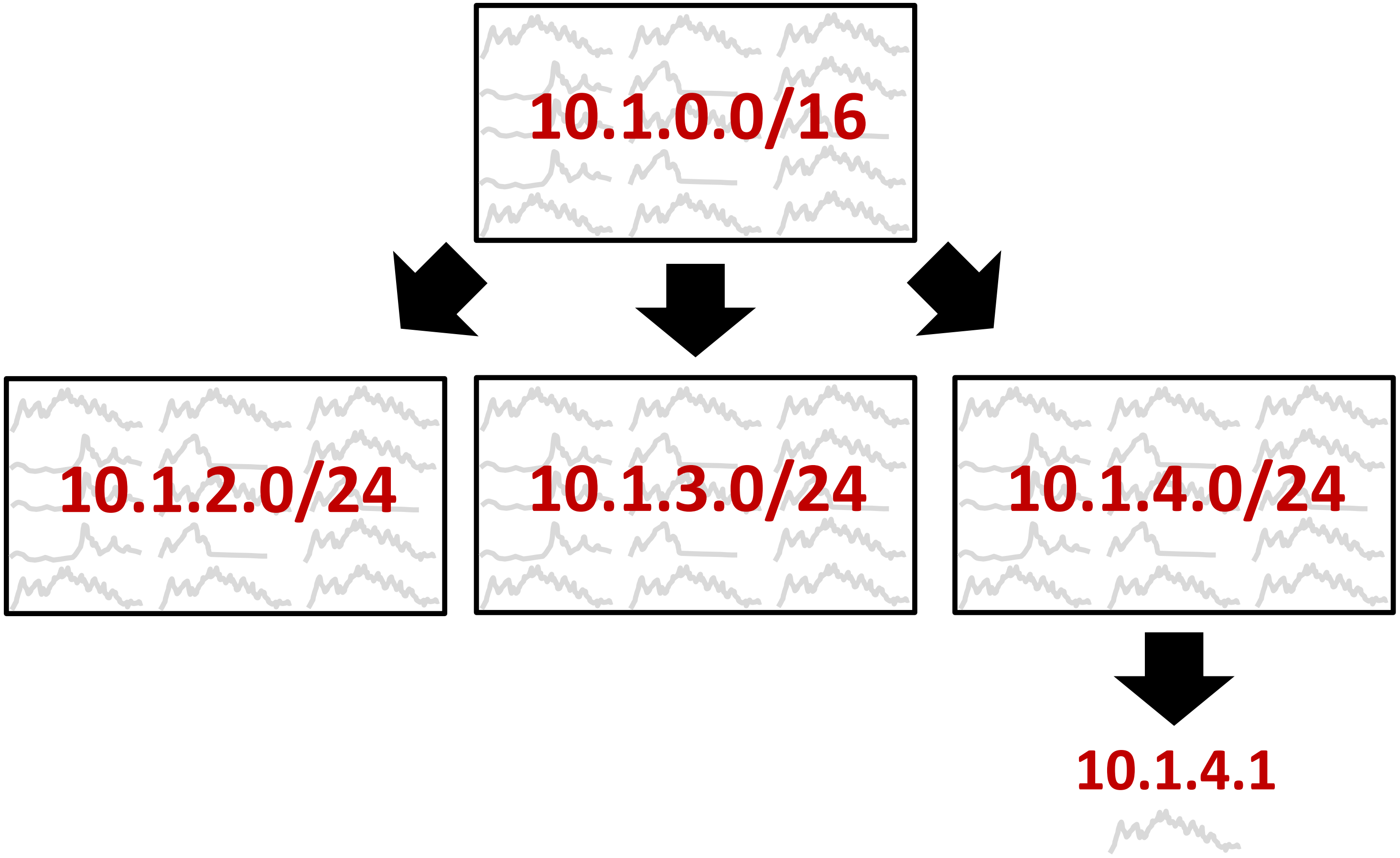
idea = 24-hour clock metaphor

each segment = 1 hour

color of segment = data value

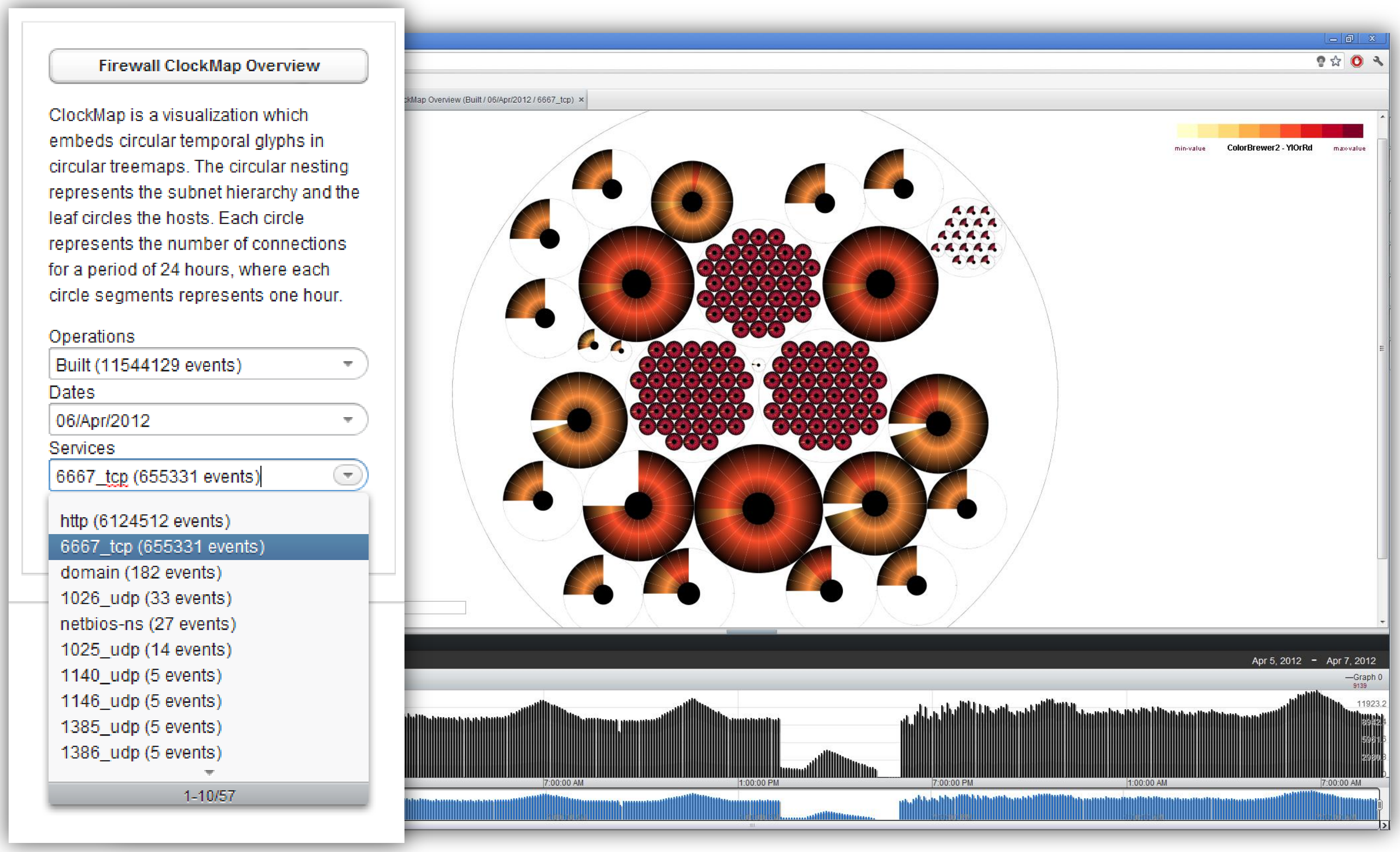
F. Fischer, J. Fuchs and F. Mansmann (2012).
ClockMap: Enhancing Circular Treemaps with Temporal Glyphs for Time-Series Data.
Proceedings of the Eurographics Conference on Visualization (EuroVis 2012 Short Papers), 2012.

Using IP Subnets as Hierarchy



ClockMap Visualization – IRC Connections

Visualizations for Firewall Connections (MC 2)



Firewall ClockMap Overview

ClockMap is a visualization which embeds circular temporal glyphs in circular treemaps. The circular nesting represents the subnet hierarchy and the leaf circles the hosts. Each circle represents the number of connections for a period of 24 hours, where each circle segments represents one hour.

Operations: Built (11544129 events)

Dates: 06/Apr/2012

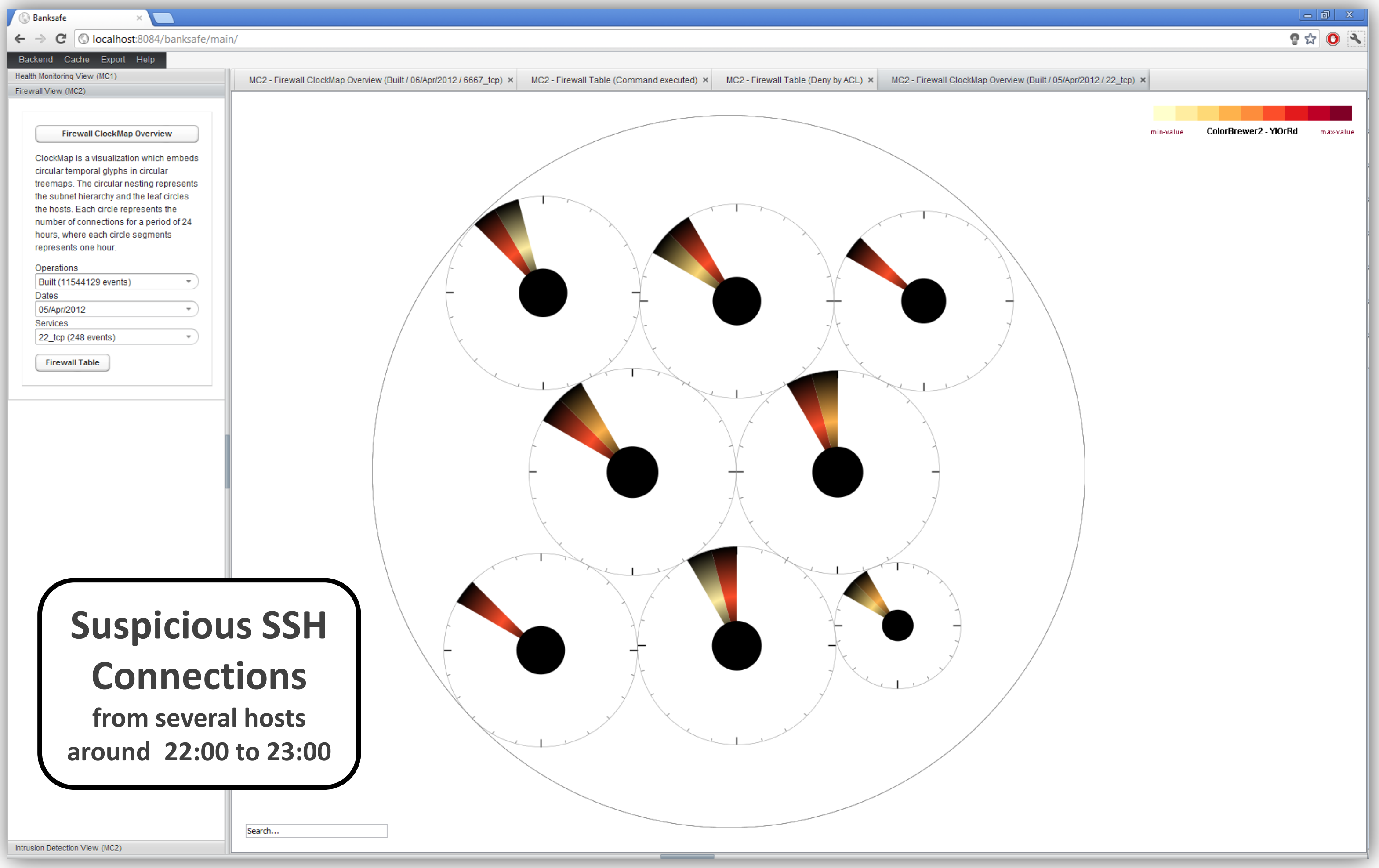
Services: 6667_tcp (655331 events)

- http (6124512 events)
- 6667_tcp (655331 events)
- domain (182 events)
- 1026_udp (33 events)
- netbios-ns (27 events)
- 1025_udp (14 events)
- 1140_udp (5 events)
- 1146_udp (5 events)
- 1385_udp (5 events)
- 1386_udp (5 events)

1-10/57

ClockMap Visualization – SSH Transmissions

Visualizations for Firewall Connections (MC 2)


Banksafe
localhost:8084/banksafe/main/
Backend
Cache
Export
Help
Health Monitoring View (MC1)
Firewall View (MC2)
MC2 - Firewall ClockMap Overview (Built / 06/Apr/2012 / 6667_tcp)
MC2 - Firewall Table (Command executed)
MC2 - Firewall Table (Deny by ACL)
MC2 - Firewall ClockMap Overview (Built / 05/Apr/2012 / 22_tcp)
Firewall ClockMap Overview
Firewall Table
min-value
ColorBrewer2 - YlOrRd
max-value
Search...
Intrusion Detection View (MC2)

ClockMap is a visualization which embeds circular temporal glyphs in circular treemaps. The circular nesting represents the subnet hierarchy and the leaf circles the hosts. Each circle represents the number of connections for a period of 24 hours, where each circle segments represents one hour.

Operations: Built (11544129 events)

Dates: 05/Apr/2012

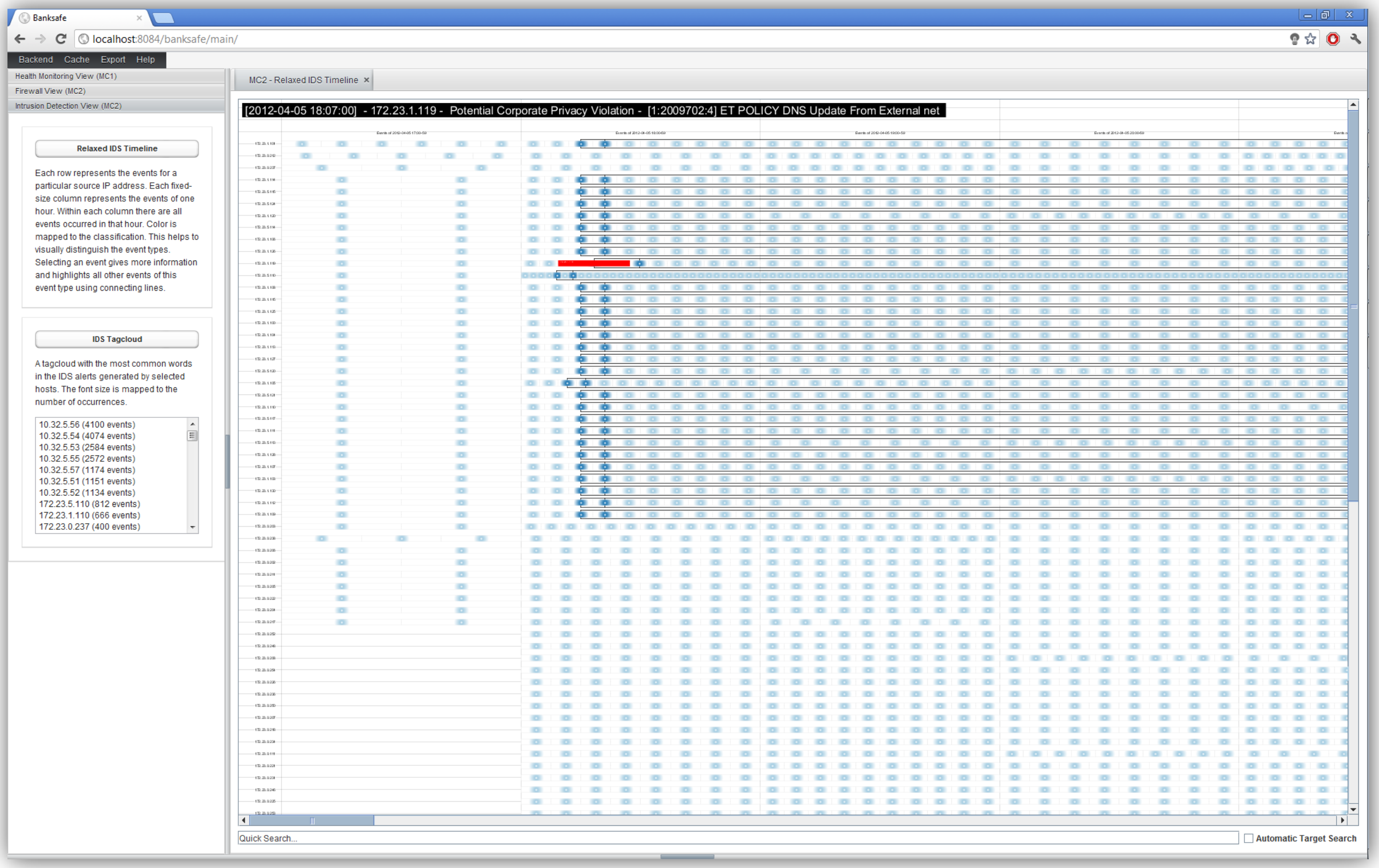
Services: 22_tcp (248 events)

Suspicious SSH Connections

from several hosts around 22:00 to 23:00

IDS Event Visualization – Overview Timeline

Visualizations for IDS Events (MC 2)



Banksafe
localhost:8084/banksafe/main/
Backend
Cache
Export
Help
Health Monitoring View (MC1)
Firewall View (MC2)
Intrusion Detection View (MC2)
MC2 - Relaxed IDS Timeline
Quick Search...
☐ Automatic Target Search

[2012-04-05 18:07:00] - 172.23.1.119 - Potential Corporate Privacy Violation - [1:2009702:4] ET POLICY DNS Update From External net

Relaxed IDS Timeline

Each row represents the events for a particular source IP address. Each fixed-size column represents the events of one hour. Within each column there are all events occurred in that hour. Color is mapped to the classification. This helps to visually distinguish the event types. Selecting an event gives more information and highlights all other events of this event type using connecting lines.

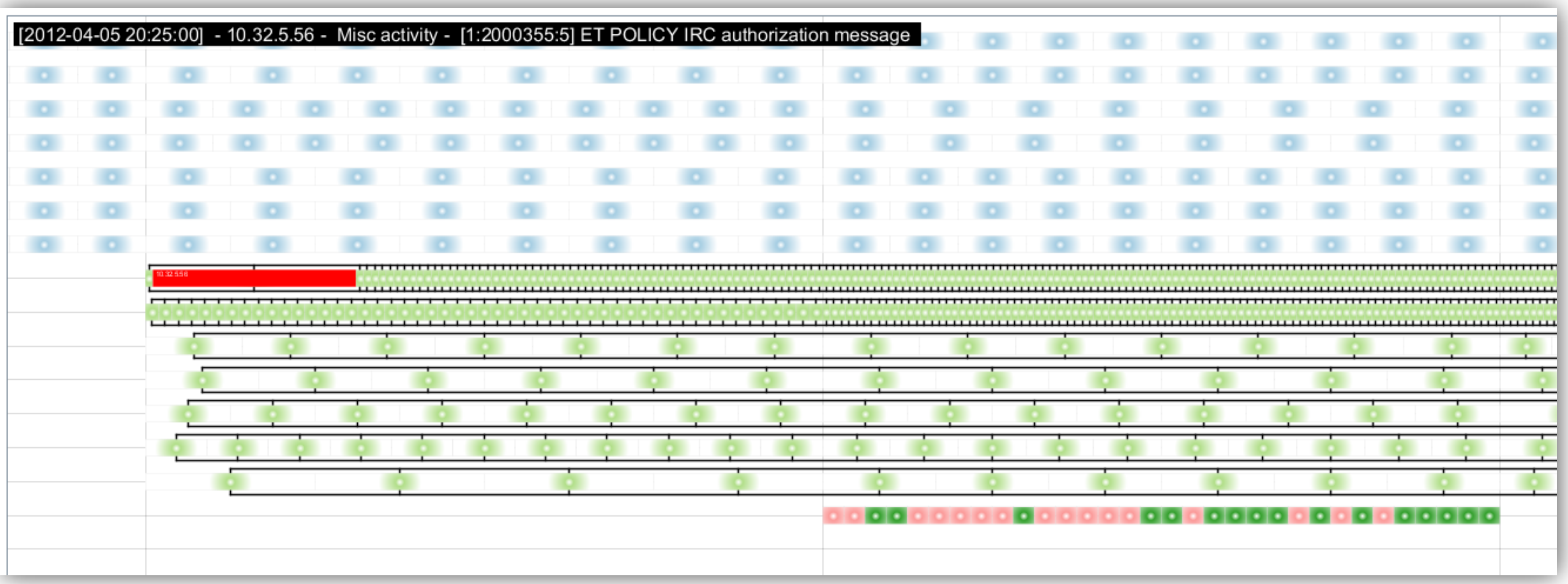
IDS Tagcloud

A tagcloud with the most common words in the IDS alerts generated by selected hosts. The font size is mapped to the number of occurrences.

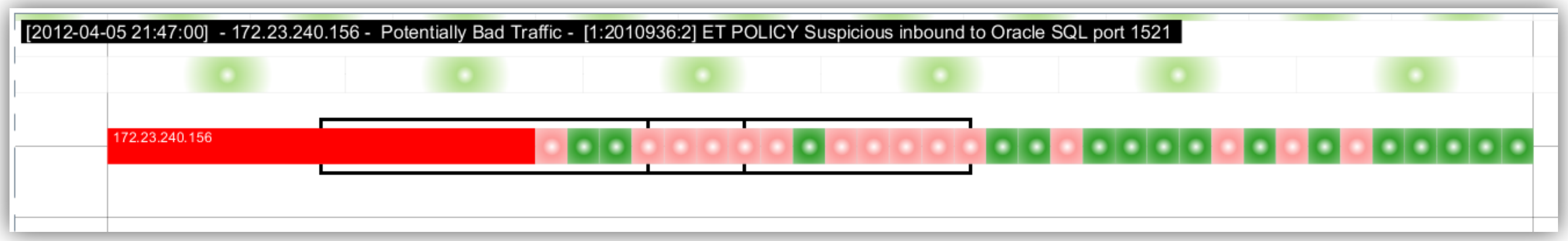
10.32.5.56 (4100 events)
10.32.5.54 (4074 events)
10.32.5.53 (2584 events)
10.32.5.55 (2572 events)
10.32.5.57 (1174 events)
10.32.5.51 (1151 events)
10.32.5.52 (1134 events)
172.23.5.110 (812 events)
172.23.1.110 (666 events)
172.23.0.237 (400 events)

IDS Event Visualization – Overview Timeline

Visualizations for IDS Events (MC 2)



[2012-04-05 20:25:00] - 10.32.5.56 - Misc activity - [1:2000355:5] ET POLICY IRC authorization message



[2012-04-05 21:47:00] - 172.23.240.156 - Potentially Bad Traffic - [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521

Lessons Learned in the Challenge

- **Backend**
  Think about infrastructure as a service (IaaS)!
  – Saves time and effort, but be aware of the issues.

For example:

`“Response too large to return.”`

This issue can occur, if you have too large intermediate queries. You should think about possible restrictions.

https://developers.google.com/bigquery/docs/query-cookbook#resultstoolarge

For example:

Reliability & Prize?

Lessons Learned in the Challenge

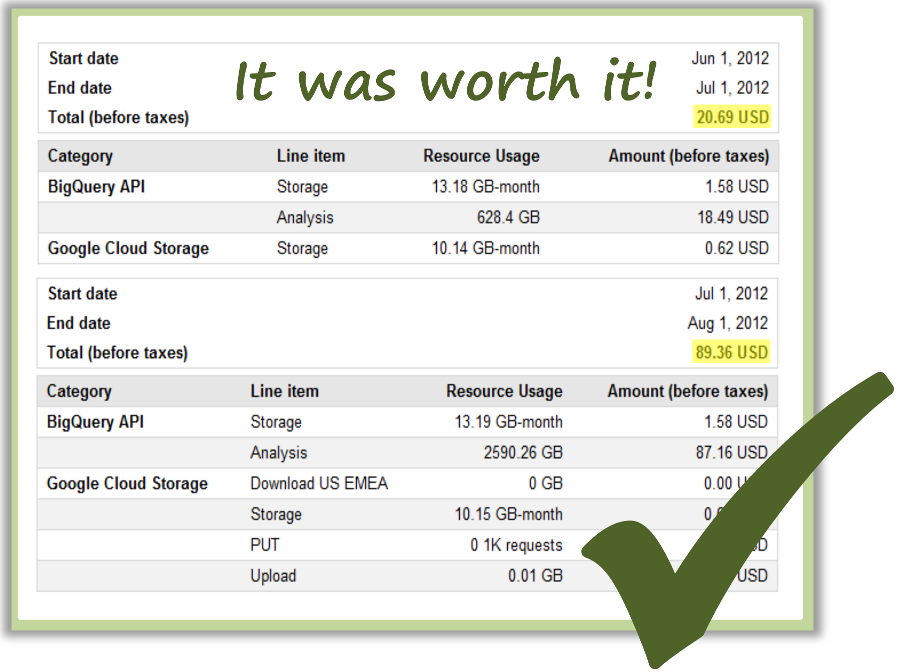
- **Backend**
  Think about infrastructure as a service (IaaS)!
  – Saves time and effort, but <u>be aware</u> of the issues.

For example:

`“Response too large to return.”`

This issue can occur, if you have too large intermediate queries. You should think about possible restrictions.

https://developers.google.com/bigquery/docs/query-cookbook#resultstoolarge



It was worth it!

Start date	Jun 1, 2012
End date	Jul 1, 2012
Total (before taxes)	20.69 USD

Category	Line item	Resource Usage	Amount (before taxes)
BigQuery API	Storage	13.18 GB-month	1.58 USD
	Analysis	628.4 GB	18.49 USD
Google Cloud Storage	Storage	10.14 GB-month	0.62 USD

Start date	Jul 1, 2012
End date	Aug 1, 2012
Total (before taxes)	89.36 USD

Category	Line item	Resource Usage	Amount (before taxes)
BigQuery API	Storage	13.19 GB-month	1.58 USD
	Analysis	2590.26 GB	87.16 USD
Google Cloud Storage	Download US EMEA	0 GB	0.00 U
	Storage	10.15 GB-month	0.
	PUT	0 1K requests	D
	Upload	0.01 GB	USD

Lessons Learned in the Challenge

- **Backend**
  Think about infrastructure as a service (IaaS)!
  – Saves time and effort, but be aware of the issues.
- **Cache**
  Think about caching!
  – Boosts performance and saves money. (e.g., EHCACHE)
- **Web Application**
  Think about web frameworks!
  – Less time needed and easier deployment. (e.g., Vaadin)
- **Combining Technologies**
  Think about combining technologies and languages!
  – We used Java Applets, but also D3.js with JavaScript.

Used Technologies

Apache Tomcat Server

Java Web Framework

Scalable Backend Database

Java Applets

Java-based persistent cache

R Scripting

Scripting Languages

Data-Driven Documents

D3.js – JavaScript Visualizations

Banksafe – Control Room

Thank you very much for your attention!

Questions?

For more information
about **BANKSAFE**
please contact

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

`http://ff.cx/`

twitter

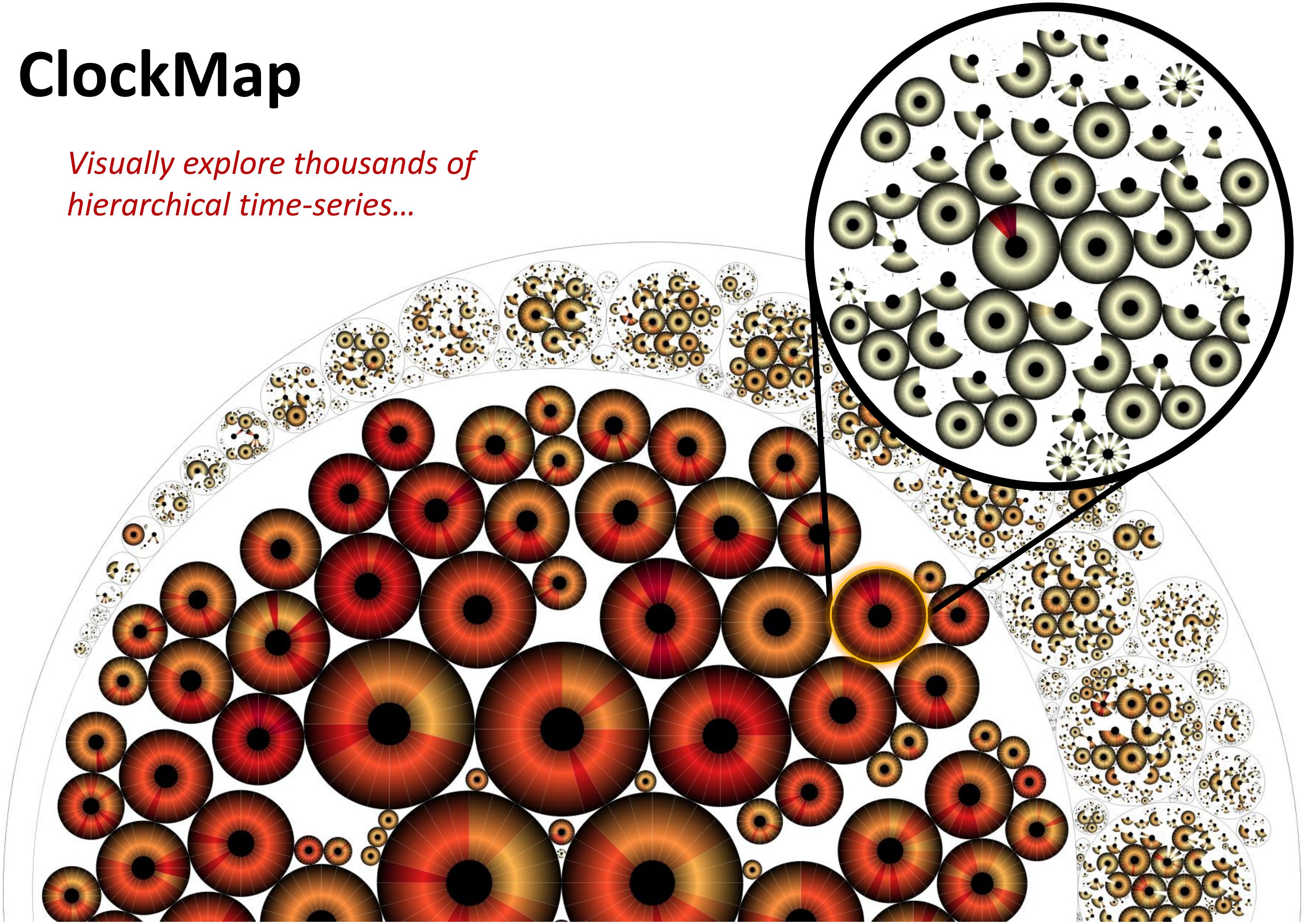
@f2cx

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.

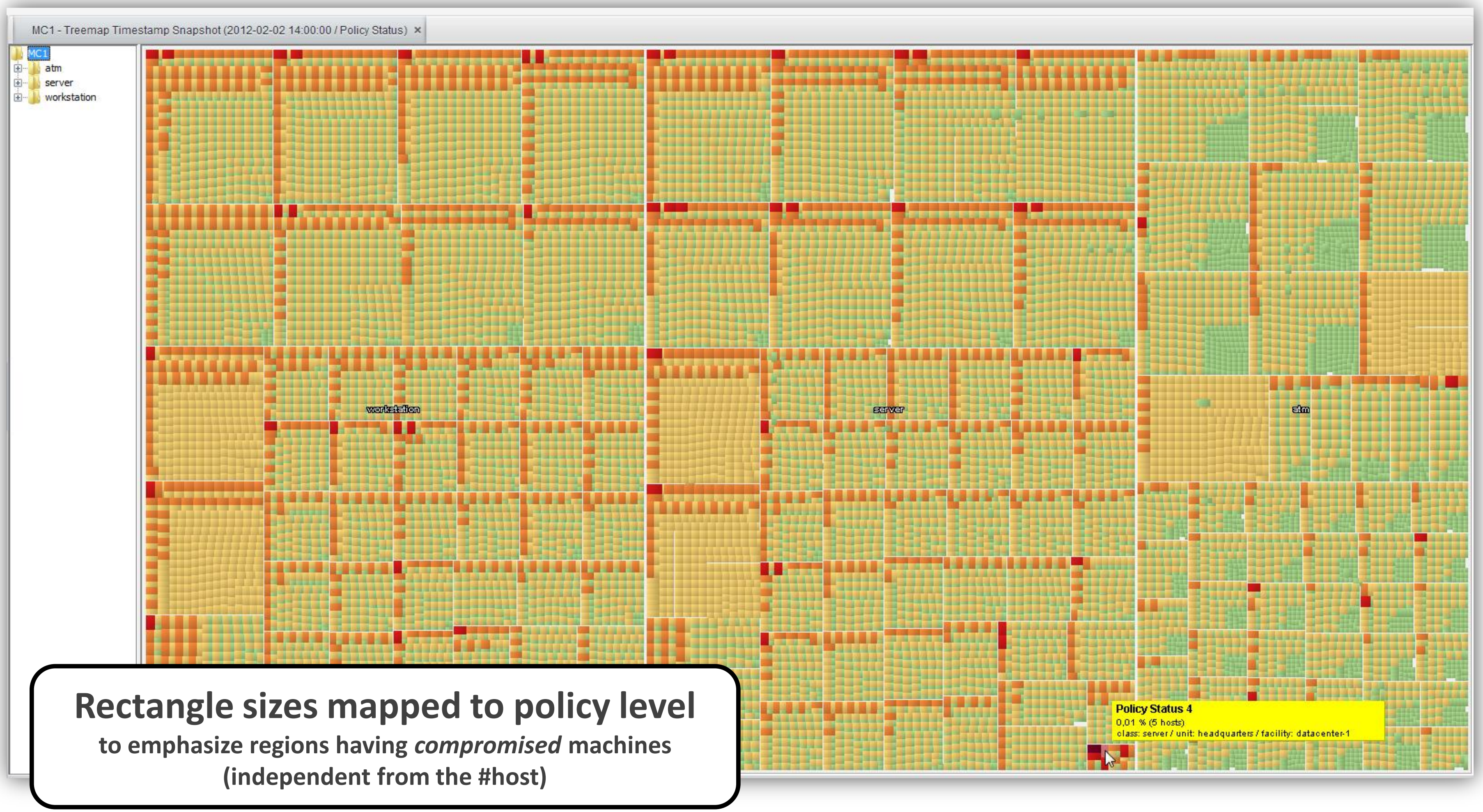
ClockMap

Visually explore thousands of hierarchical time-series…



Point-in-Time Health Overview

Visualizations for Health Monitoring (MC 1)



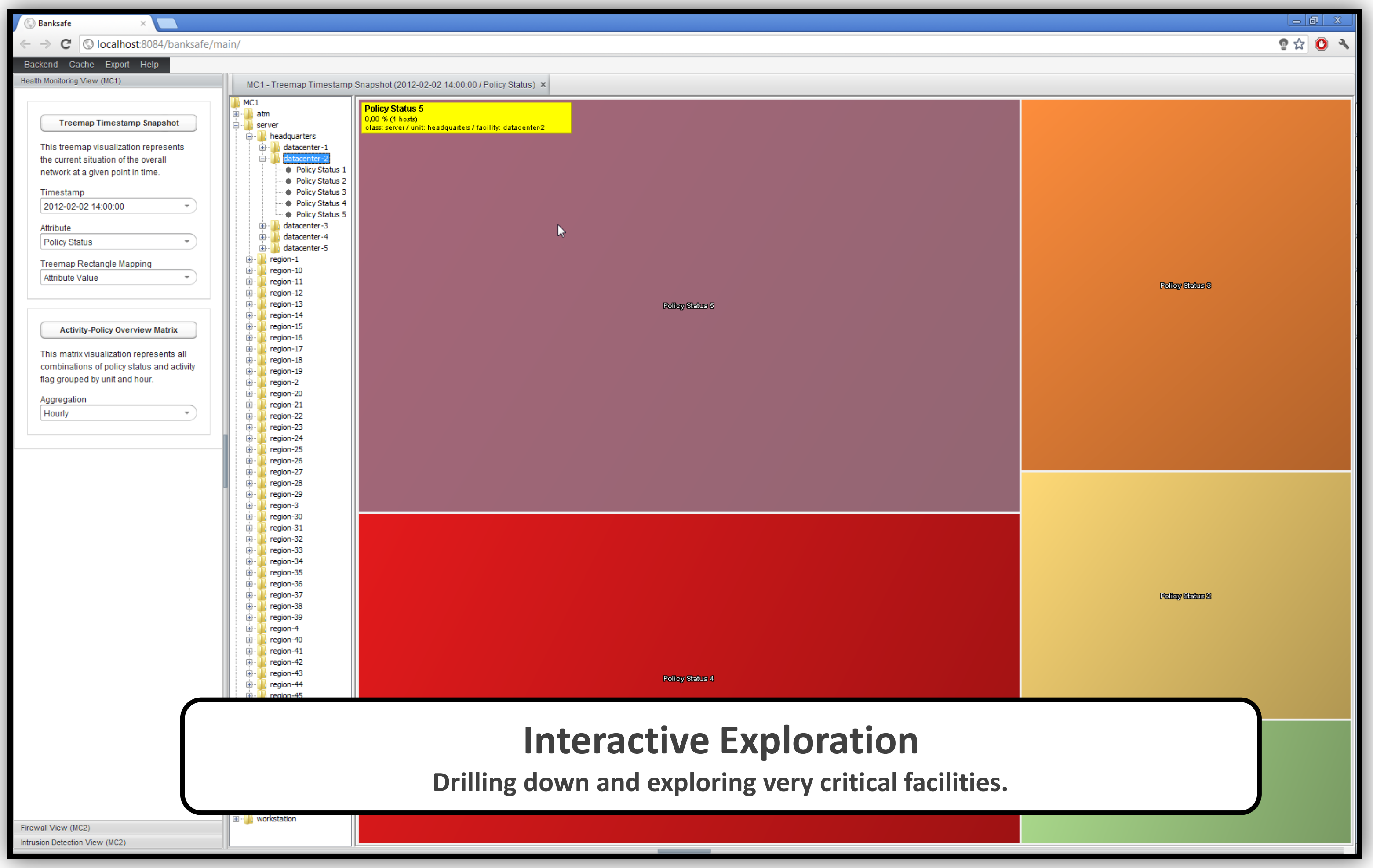
MC1 - Treemap Timestamp Snapshot (2012-02-02 14:00:00 / Policy Status)

Policy Status 4
0,01 % (5 hosts)
class: server / unit: headquarters / facility: datacenter-1

Rectangle sizes mapped to policy level
to emphasize regions having *compromised* machines
(independent from the #host)

Point-in-Time Health Overview

Visualizations for Health Monitoring (MC 1)



This treemap visualization represents the current situation of the overall network at a given point in time.

Timestamp: 2012-02-02 14:00:00

Attribute: Policy Status

Treemap Rectangle Mapping: Attribute Value

This matrix visualization represents all combinations of policy status and activity flag grouped by unit and hour.

Aggregation: Hourly

Policy Status 5
0,00 % (1 hosts)
class: server / unit: headquarters / facility: datacenter-2

Interactive Exploration

Drilling down and exploring very critical facilities.