PANOPTESEC
An FP7 ICT Project

Objective ICT-2013.1.5 Trustworthy ICT (Item c)

Giuseppe Santucci

Dipartimento di Informatica e Sistemistica

Sapienza Università di Roma

santucci@dis.uniroma1.it

La Habana, 19.02.2014

Outline

- Overview of the Panoptesec Project
- Details of Panoptesec architecture
- Panoptesec WP6 (Visualization - Visual Analytics)
  - Lessons learned by previous activities
  - Up to date example of cybersecurity tools (commercial+research)
  - Design methodology

FP7 Objective

- Objective ICT-2013.1.5 Trustworthy ICT

  c) Development, demonstration and innovation in cyber security

  "This activity addresses the application of technologies to ***increase the level of cyber security*** in Internet. This includes the development and demonstration of technologies, methodologies and processes to ***prevent, detect, manage and react*** to cyber incidents in real-time, and to support the breach notifications, improving the ***situational awareness*** and supporting the ***decision making*** process. It will also develop and demonstrate advanced technologies and tools that will empower users, notably individuals and SMEs, in ***handling security incidents*** and ***protecting their privacy***."

PANOPTES figures

- The total budget of the project is approximately 7,5 million € and the European Commission is funding 70%
- START September 2013
- STOP September 2016
- The project full title is “Dynamic Risk Approaches for Automated Cyber Defence” and will be completed in 2016
- Just a note about European projects…

PNOPTESEC Consortium (8 PARTNERS)

1. Institut Mines-Telecom (IMT) **France** - A group of prestigious **higher education** establishments under the Ministry of Industry will coordinate the overall project
2. RHEA **Belgium** - A software and engineering **consulting company** specialising in space and other cutting-edge technologies, for the technical organisation and monitoring of the technical progress.
3. Alcatel-Lucent Bell Labs **France** - A **research company** of optical components, networks architectures and data analytics,
4. Epistematica **Italy** – A company operating in the **market of IT services** and software applications
5. The Research Center of Cyber Intelligence and Information Security (CIS) **Italy** - Cis belongs to Sapienza **University of Rome**, which is one of the largest and oldest universities in Italy
6. The Hamburg University of Technology (TUHH) **Germany** - A **young university** with a 10-year involvement in technology for ontologies,
7. SUPELEC **France** – One of the most famous and prestigious **higher education institutes** of engineering
8. ACEA **Italy** – **Energy and water provider** in Rome. It will provide the test bed for the project

Research Proposal - Objectives

ICT-2013.1.5 Item (c) Objectives	PANOPTES Objective	Measure of Effectiveness
Prevent cyber incidents in real-time	Proactively calculate risk, identify and actuate courses of action based on evaluated operational impact due to updated knowledge of cyber vulnerabilities and changes in network and computer system configuration.	Improve course of action determination time **from days to minutes**.
Detect cyber incidents in real-time	Provide multi-sensor data integration and correlation of infrastructure, security and operations data through the use of advanced ontology and inference technologies.	Reduce detection false positive rate **by 25%**. Reduce detection false negative rate **by 25%**.
Manage cyber incidents in real-time	Reactively calculate risk, identify and actuate courses of action in a fully automated manner, based on evaluated operational impact due to detected cyber incidents.	Fully integrated system from **detection to automated response**.
React to cyber incidents in real-time	Recommend reactive courses of action optimized to maximally deny attacker capabilities while minimizing operational impact. Actuate reactive courses of action (**optionally**) in fully automatic mode.	Reduce cyber incident response time **from hours to seconds**.
Support attack notifications	Provide optimized notification of detected cyber incidents through the use of advanced technologies for multi-sensor data integration and correlation.	Reduce detection false positive rate **by 25%**. Reduce detection false negative rate **by 25%**.

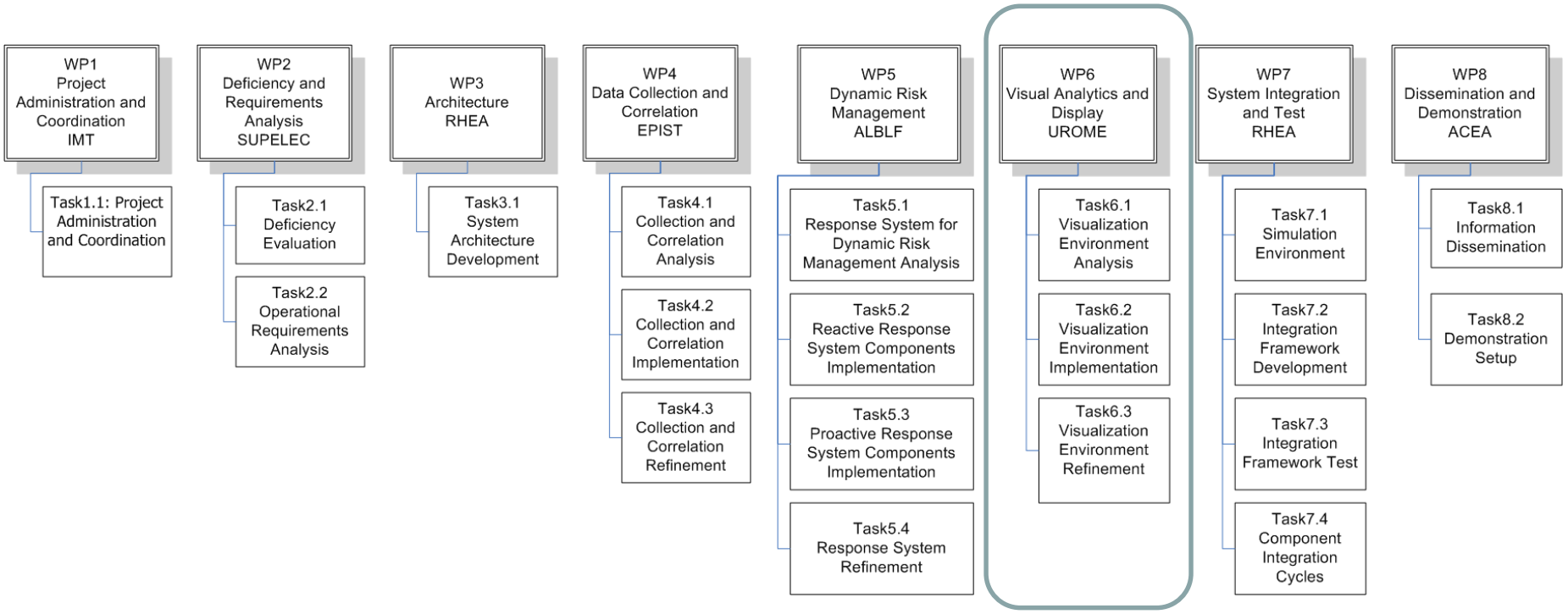
Research Proposal - Objectives

ICT-2013.1.5 Item (c) Objectives	PANOPTES Objective	Measure of Effectiveness
Improve situational awareness	Provide an **advanced visual analytics engine** to improve security operator's ability to access and analyze large complex data sets.	Reduce operator analysis time **from days to minutes**.
Support decision-making process	Develop proactive and reactive risk and response models to provide optimized course of action recommendations to operators.	Identified course of action responses **do not adversely affect operations**.
Develop advanced technologies and tools	Deliver an integrated system of beyond-stated-of-the-art cyber security algorithms and software modules providing continuous monitoring and automated response for cyber defence.	Fully integrated system from **detection to automated response**.
Demonstrate advanced technologies and tools	Conduct demonstrations on operational segment of user agency network (ACEA) for comparison of PANOPTES-delivered capabilities against status quo.	Demonstrate improved operational response in **operational environment**.
Empower users in handling security incidents (SMEs)	Deliver an integrated system for cyber security detection and response scalable for use by both SMEs and larger enterprises.	Demonstrate scalability of system in range **from 10 nodes to 10,000 nodes**.

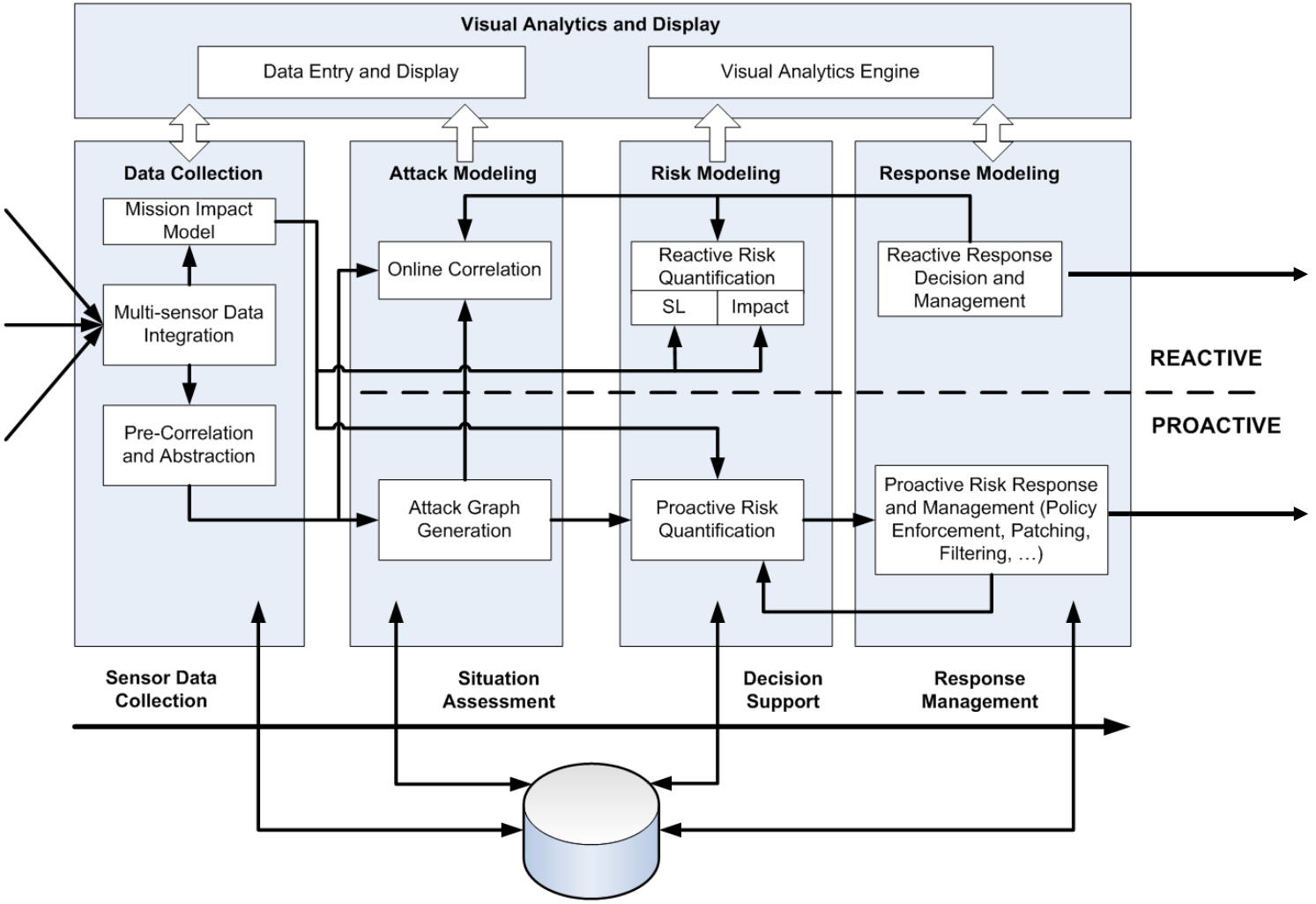
Activities/Phases

- **Preliminary Requirements and Design:** This phase is used to conduct an overall assessment of cyber defence systems currently in use by ACEA and user agencies from across several sectors to evaluate their deficiencies.
- **Component Analysis and Design:** This phase includes iterative process of component-level detailed requirements definition and design.
- **Component Implementation and Test:** This phase involves the iterative evolution of component-level prototypes to meet the functional requirements.
- **Component Experiments and Refinement:** This phase provides the opportunity for component-level prototypes to undergo experiments and further functional refinement.
- **System Integration and Test:** This phase collects the refined integration-level prototypes and incorporates them into a complete system.
- **System Demonstration:** This phase involves integrating the system into the operational environment.

Work Packages

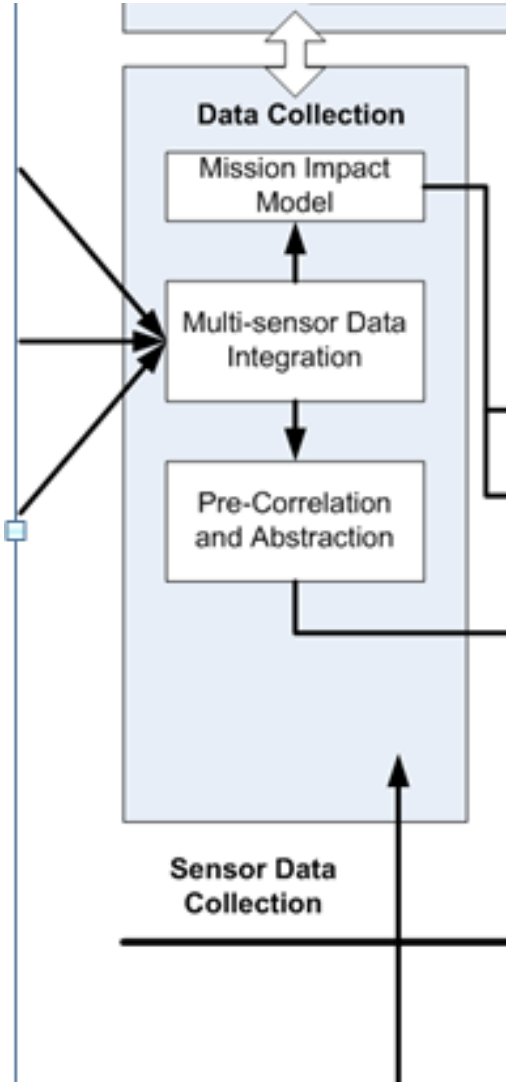


Architecture



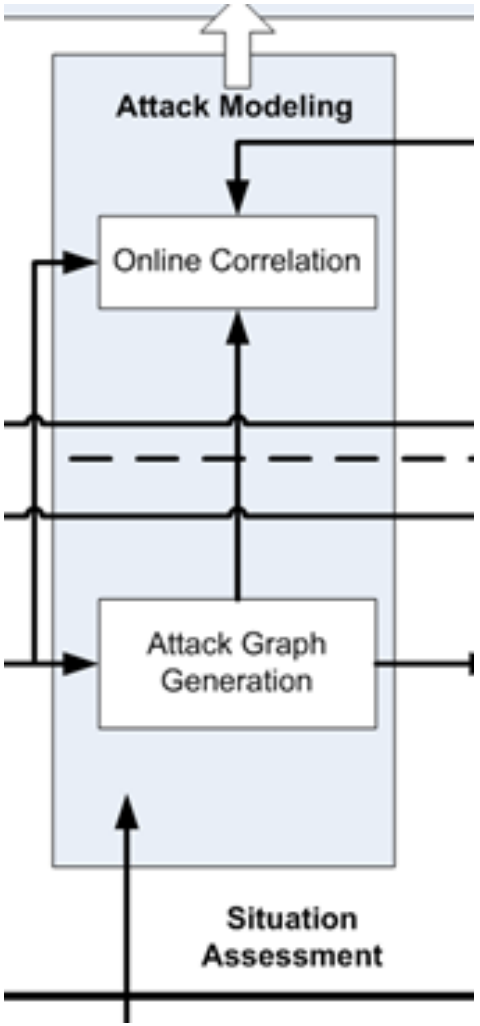
Data collection

- **Mission Impact Model:** ensures that the relationship between priority operational capabilities and the supporting infrastructure services or systems are captured. The model captures the operational knowledge of the priority goals to protect by relating operational capability to the dependent infrastructure services or systems. Similarly, the model also captures the impact that courses of action intended to mitigate cyber security issues may have on the ability of an organisation to carry out their mission.
- **Multi-sensor Data Integration:** provides the interfaces needed to collect security relevant data from infrastructure and non-infrastructure data sources, fusing the data into a common model.
- **Pre-correlation and abstraction:** performs pre-correlation to merge data sets from multiple sensors into a single data model using semantic inference engines.



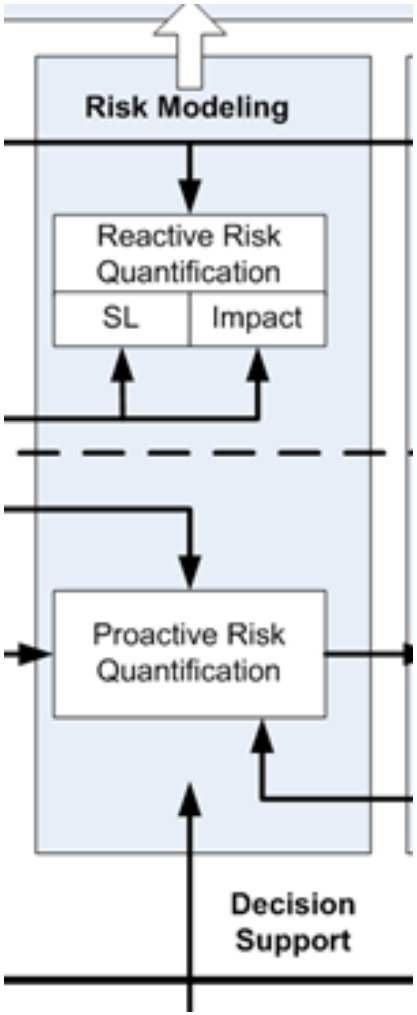
Situation assessment

- **Online Correlation:** matches pre-computed attack paths with real-time cyber security incident data to identify potential next-stage attack points between the identified incident and priority goals to protect
- **Attack Graph Generation:** calculates possible attack paths based on infrastructure configuration information (e.g., data path connectivity and system configurations including running software and services) and reference cyber security data (e.g., software vulnerabilities). Attack paths are calculated from hypothetical attack sources to priority goals to protect



Decision support

- **Reactive Risk Quantification:** calculates the risk associated with the priority mission goals to protect, based on the system knowledge of ongoing cyber security incidents
- **Proactive Risk Quantification:** calculates the risk associated with the priority mission goals to protect, based on the identified system and service value to the mission, knowledge of threat likelihood and presence of vulnerabilities

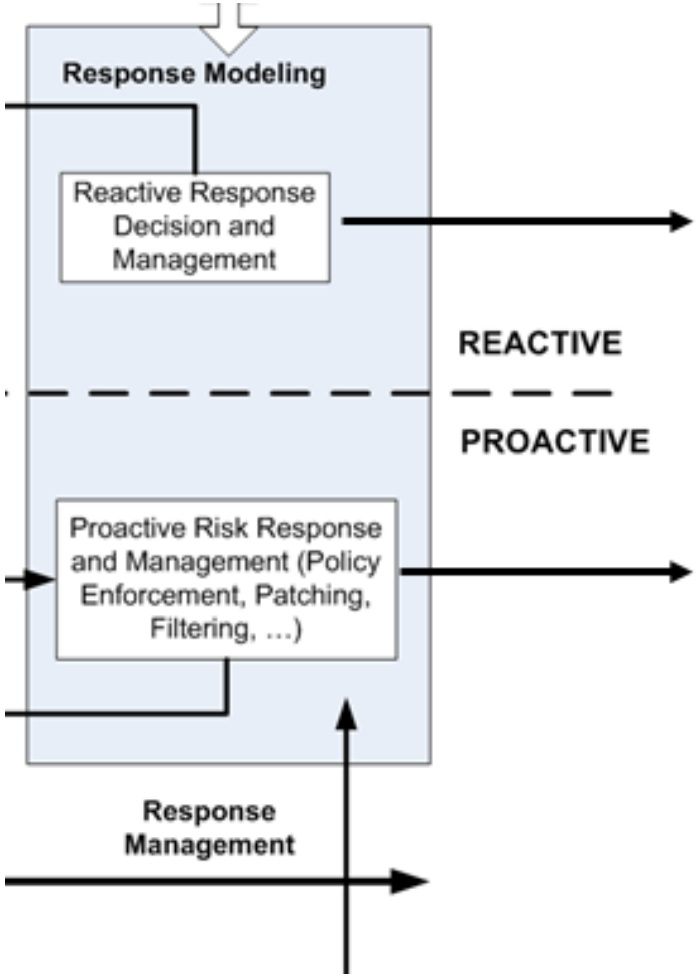


Reactive

Proactive

Response management

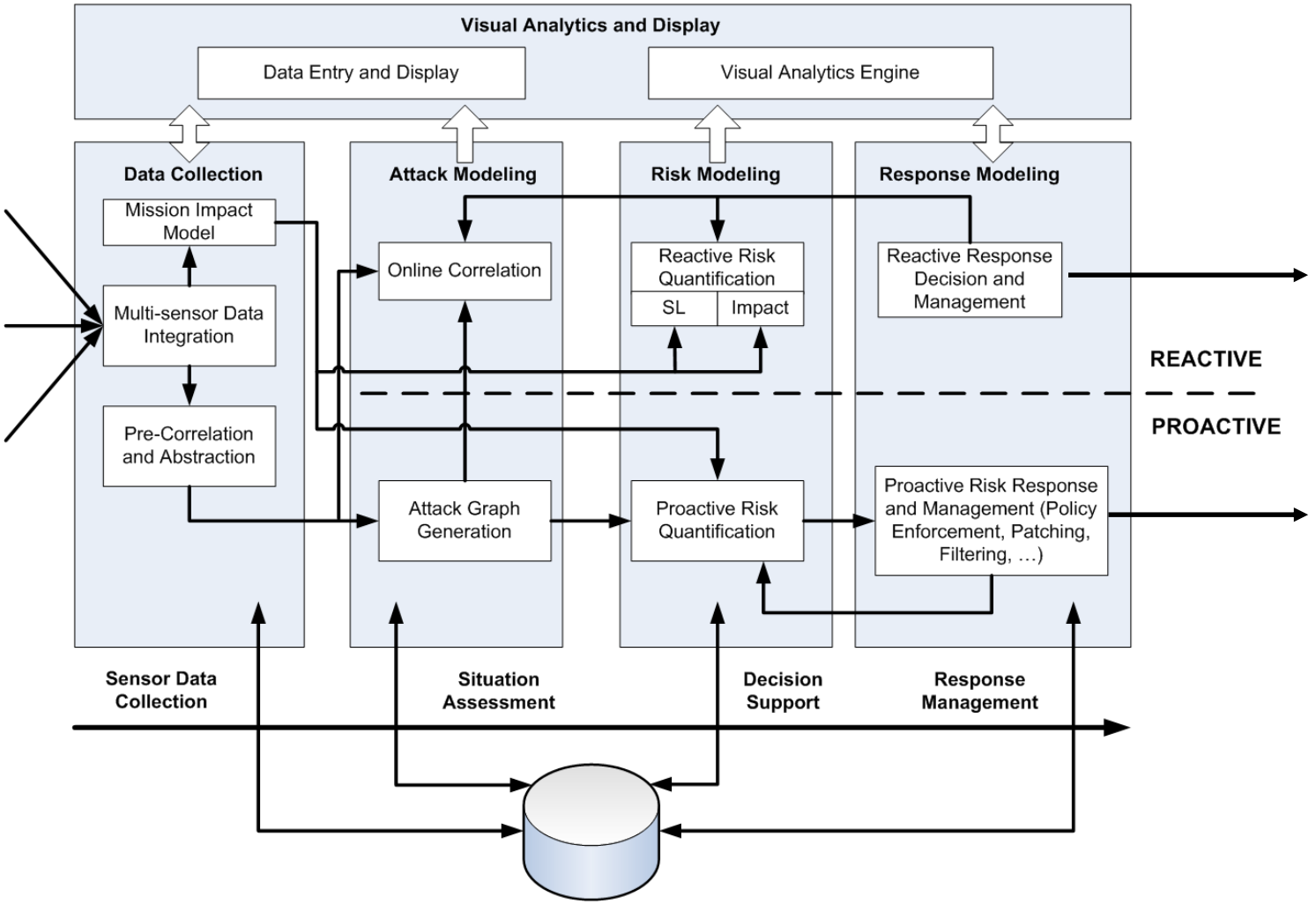
- **Proactive Risk Response and Management:** calculates the optimal courses of action in response to calculated attack paths due to vulnerabilities and resulting operational risk
- **Reactive Response Decision and Management:** calculates the optimal courses of action in response to calculated attack paths due to vulnerabilities, presence of ongoing cyber attacks and resulting operational risk



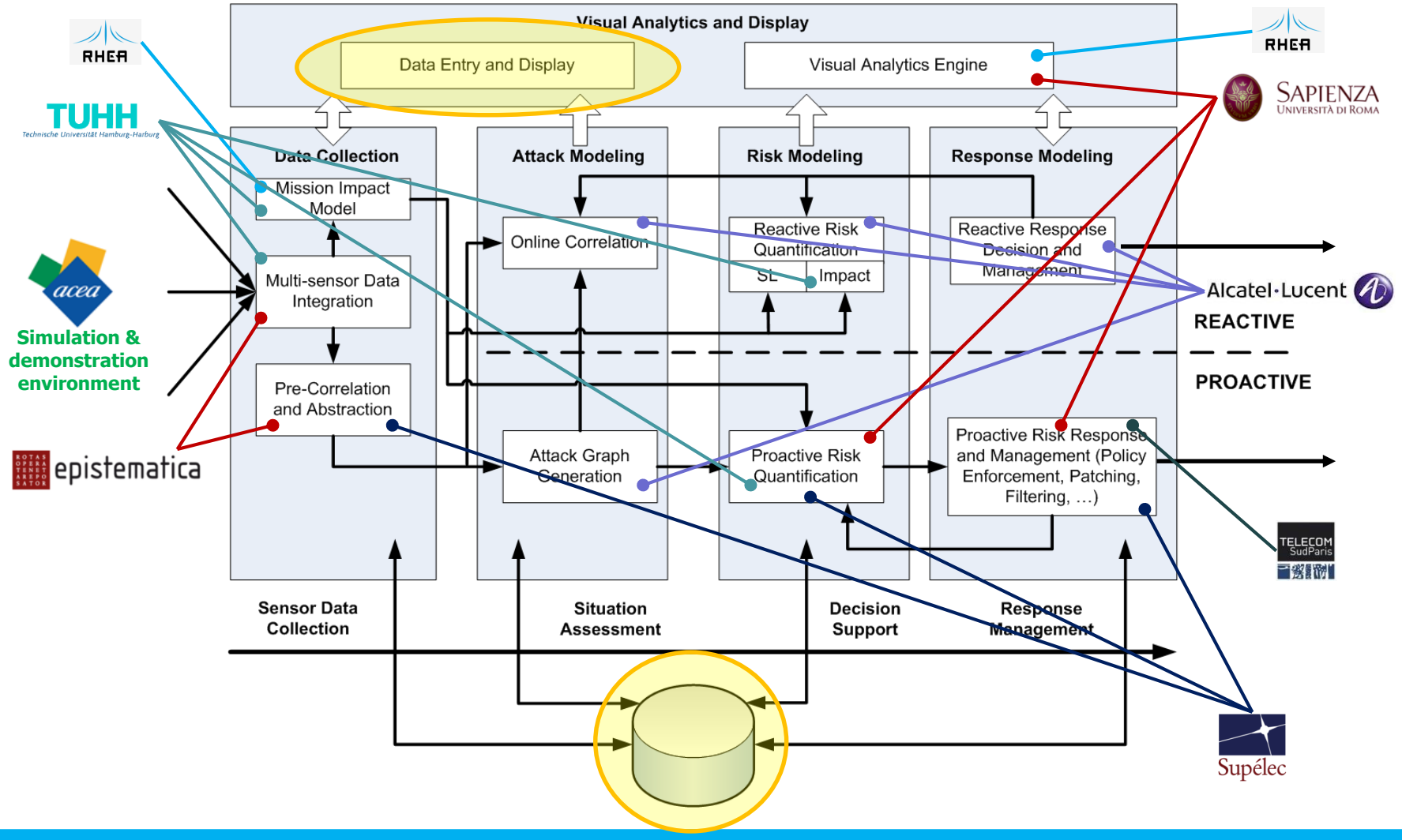
Visual analytics

- **Data Entry and Display:** provides the general display environment enabling the operator to interact with the various modules supporting the operational flow.
- **Visual Analytics Engine:** provides the operator with access to all data within the database for deep analysis.

Architecture



Participant contributions



WP6 Visual analytics and display

- WP6 Visual analytics and display (CIS-UROME) (months 4-31)
  - Task 6.1 Responsible: CIS-UROME; Participants: RHEA, EPIST, CIS-UROME, ACEA, SUPELEC
  - **Detailed requirements and design reports**
  - Task 6.2 Responsible: CIS-UROME; Participants: RHEA, EPIST, CIS-UROME, ACEA, SUPELEC
  - **Component first prototypes - Integration ready prototypes**
  - Task 6.3 Responsible: CIS-UROME; Participants: RHEA, EPIST, CIS-UROME, ACEA, SUPELEC
  - **Integration ready prototypes**
  - **Prototype reports**

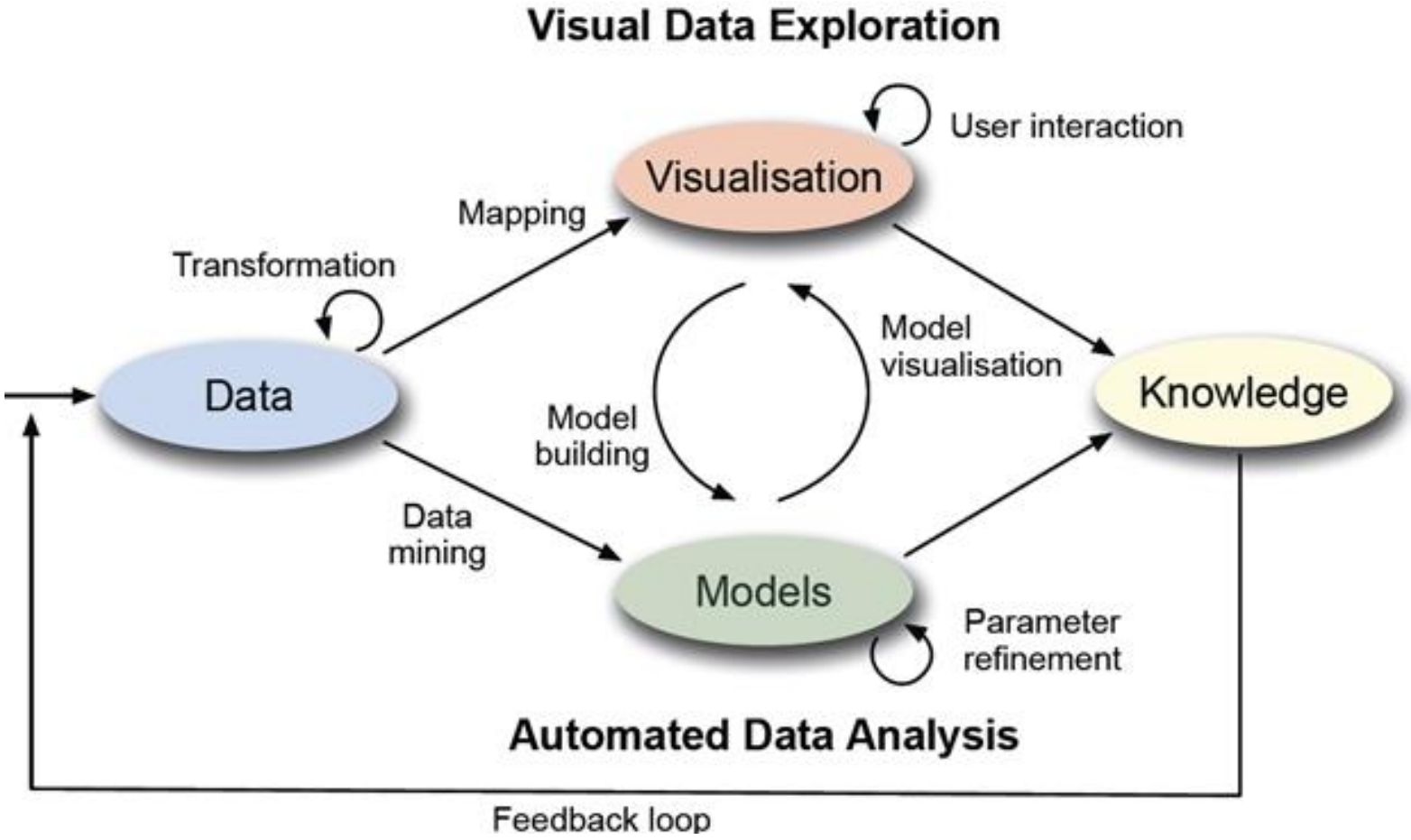
It is a hard task to deal with

- Panoptesec analysis
  - Mission Impact Model
  - Attack Graph Generation
  - Online Correlation
  - Proactive Risk Quantification
  - Reactive Risk Quantification
  - Proactive Risk Response and Management
  - Reactive Response Decision and Management

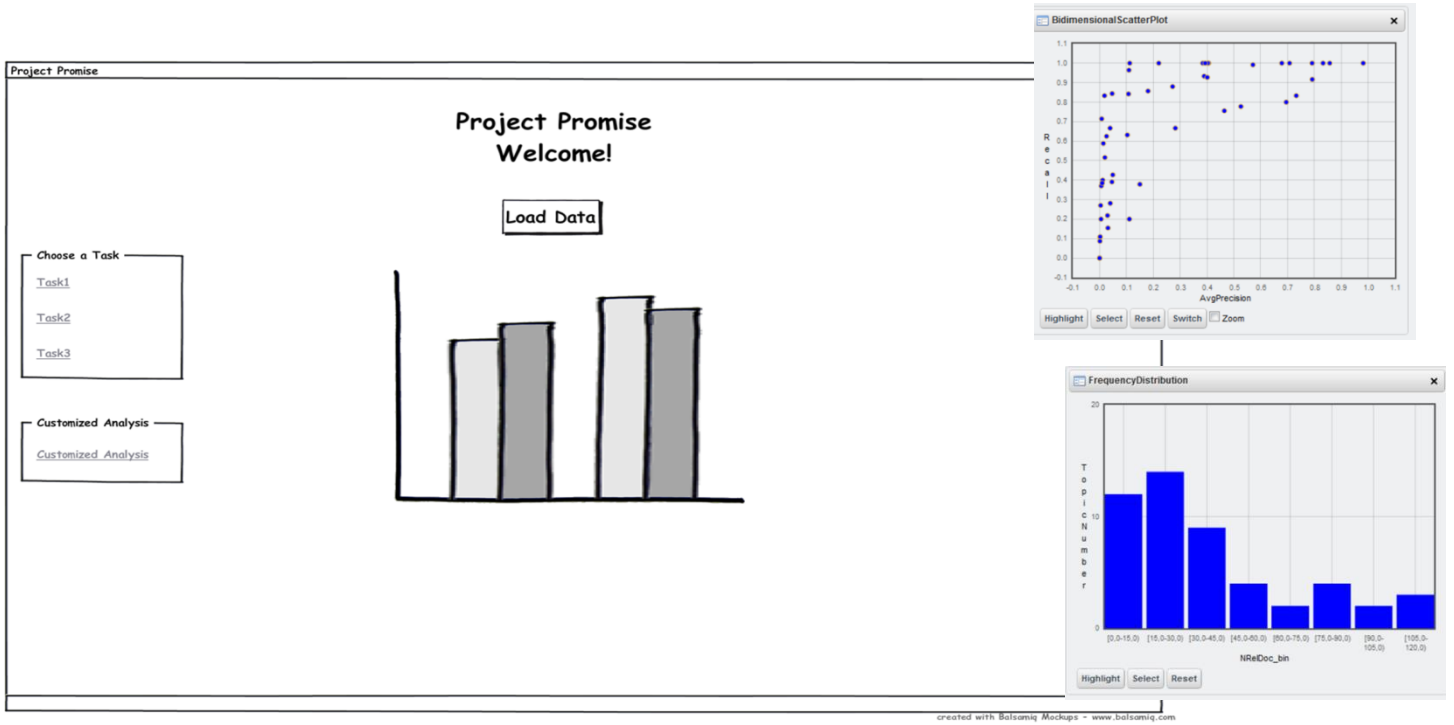
How to do that?

- Some issues coming from a successful European project ended on 2013 (PROMISE) about information retrieval (IR) evaluation
- In a nutshell, evaluating an IR system produces hundreds of metrics that must be inspected (VISUALIZED !) to assess:
  - Retrieved documents
  - Ranking

A clear methodology

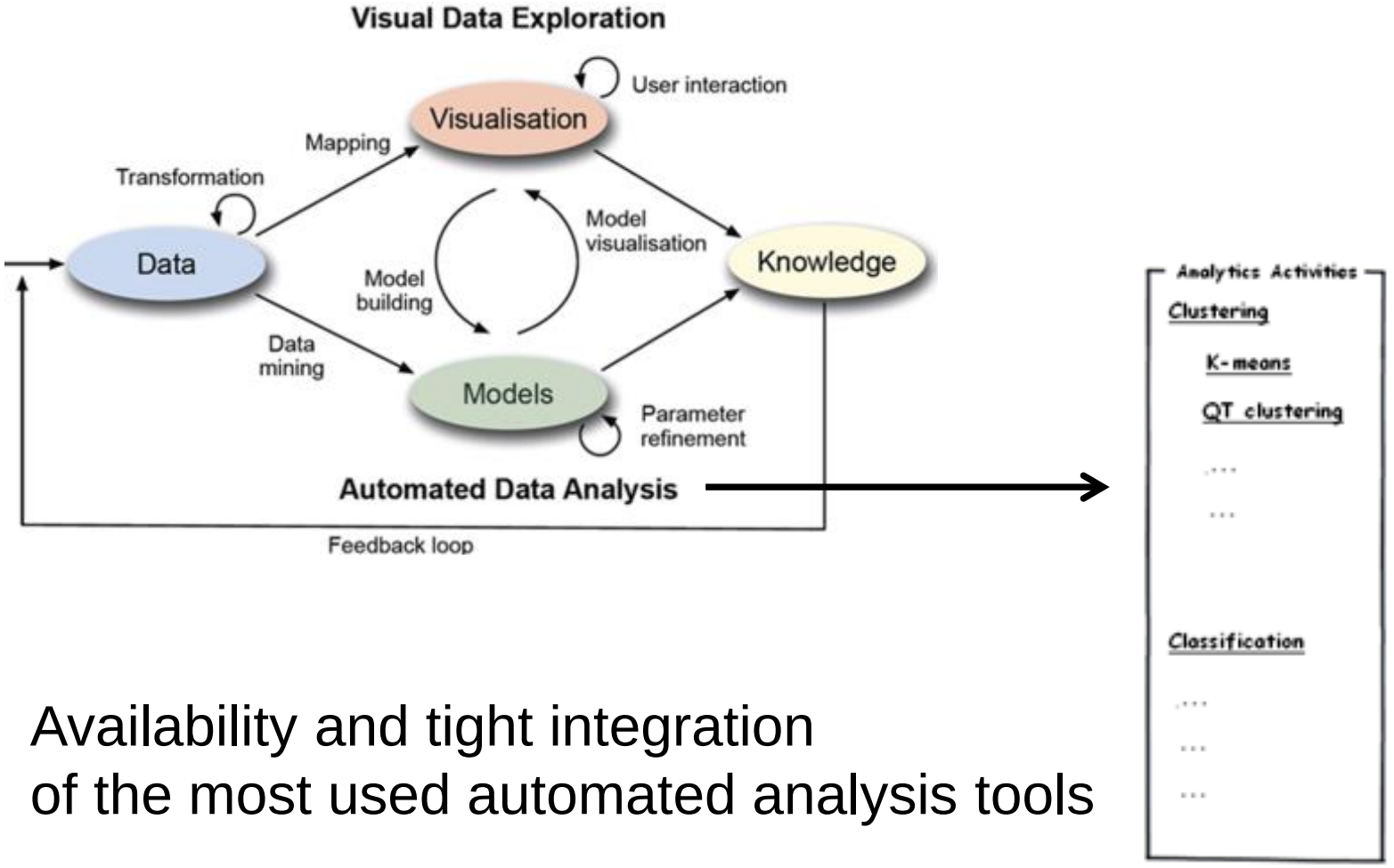


Automation



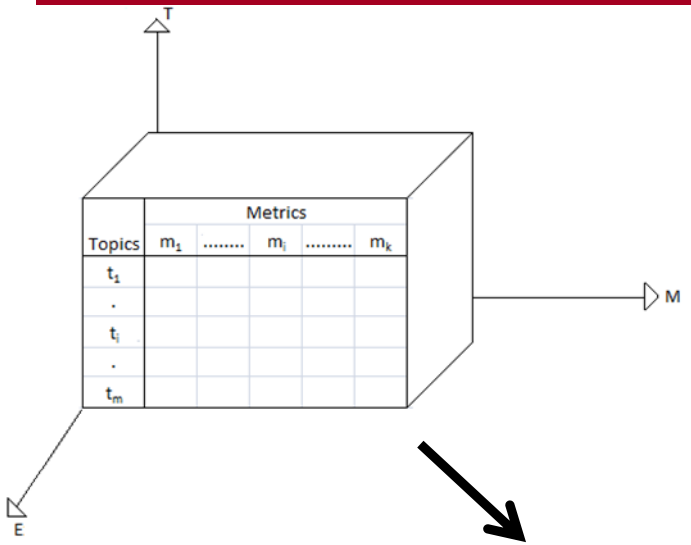
- Visualizations MUST BE integrated within the system and are automatically generated

Automated data analysis integration



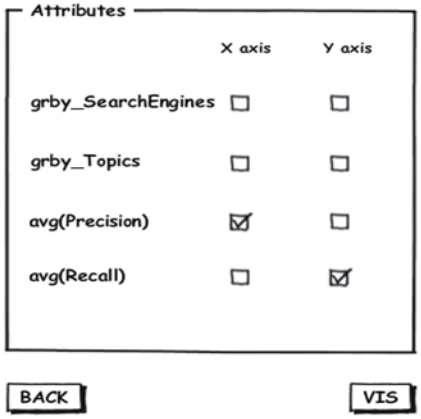
Availability and tight integration
of the most used automated analysis tools

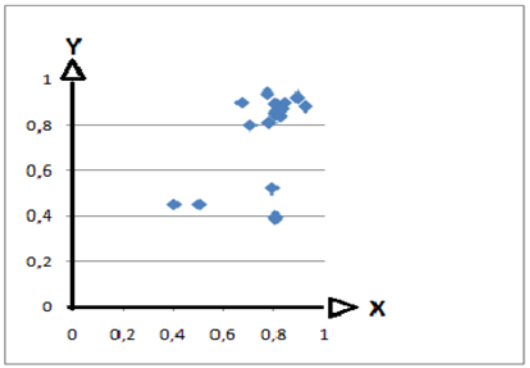
Formal mapping between data & visualization



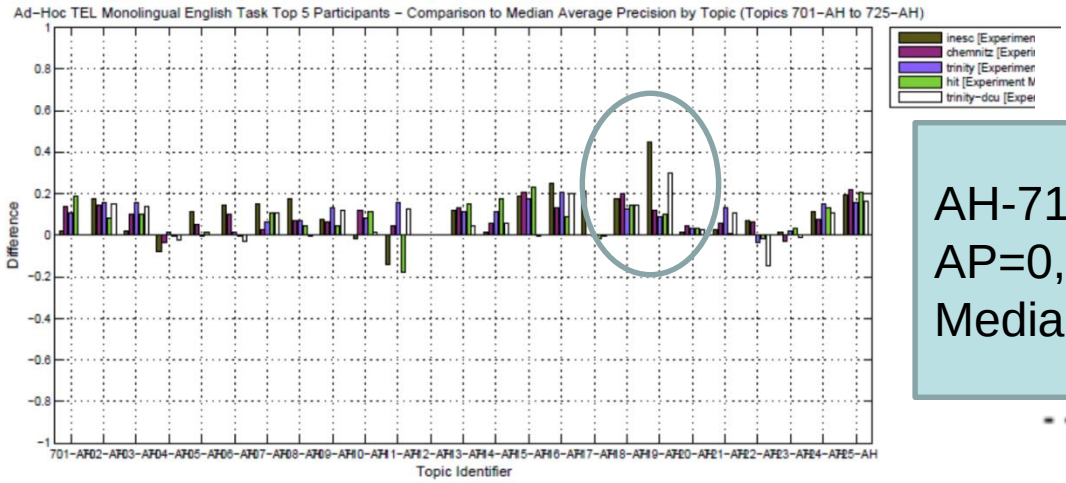
Understand the user data before visualize it!!!

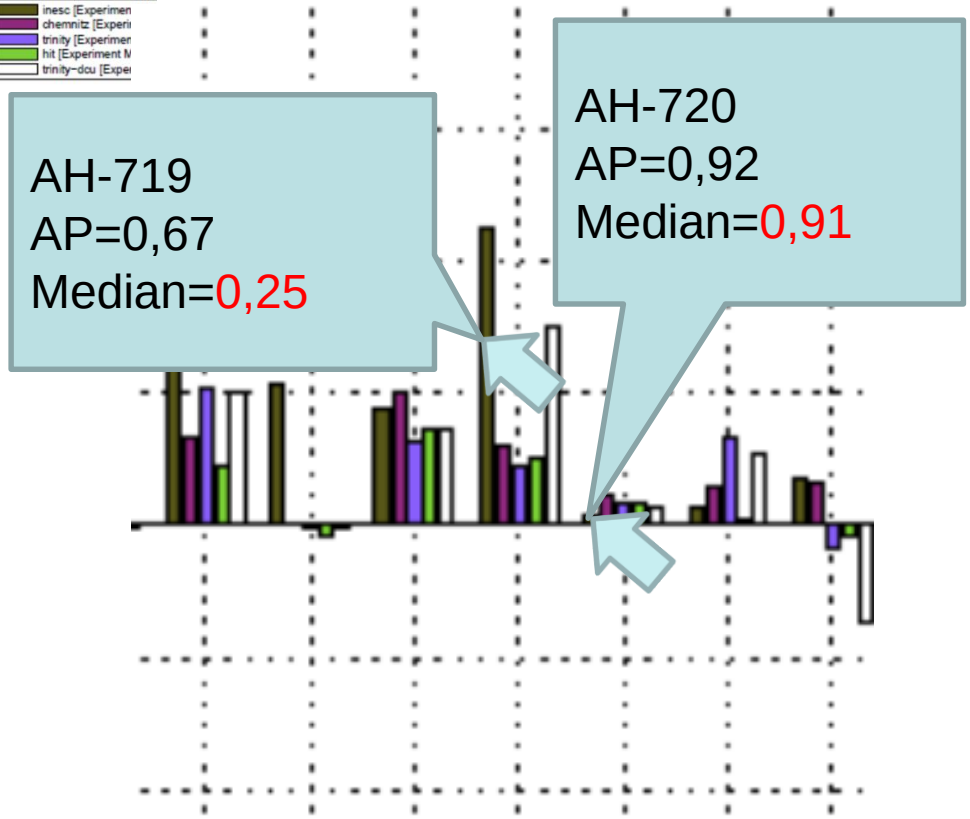
Mapping
Scatterplot





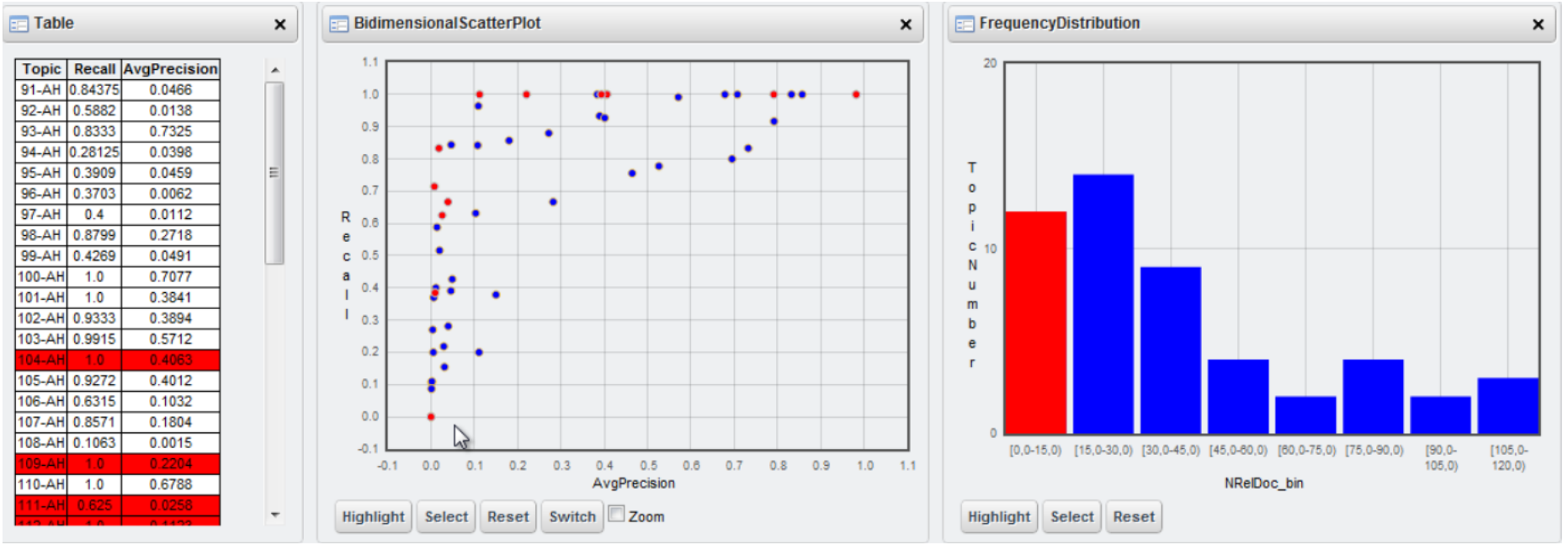
Interaction



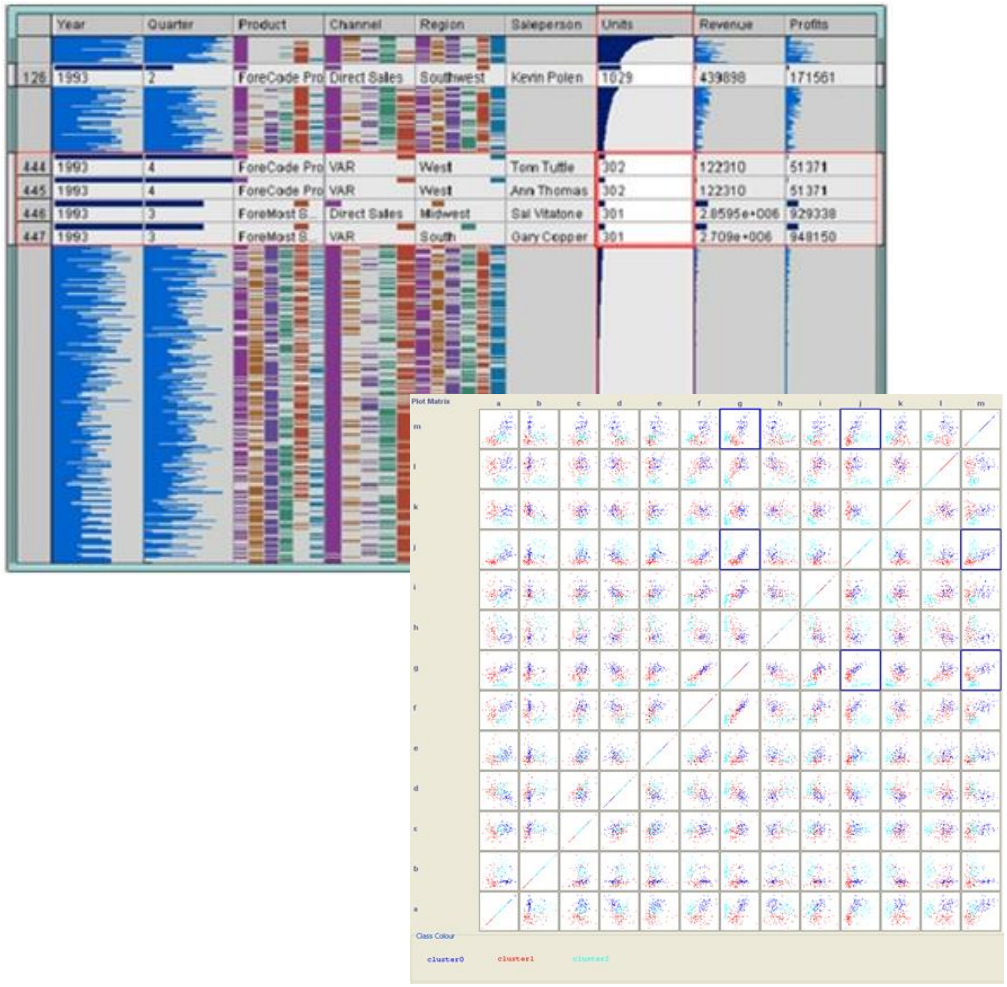


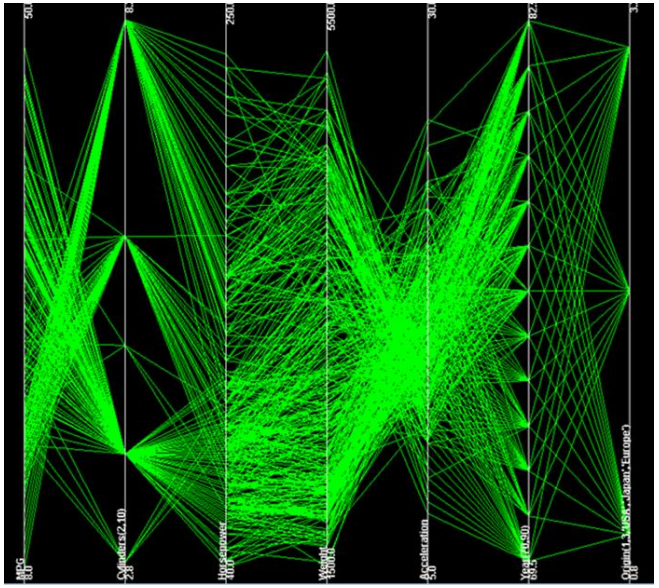
Zoom in/out
Reordering,
Brushing,
...

Parallel and coordinated views



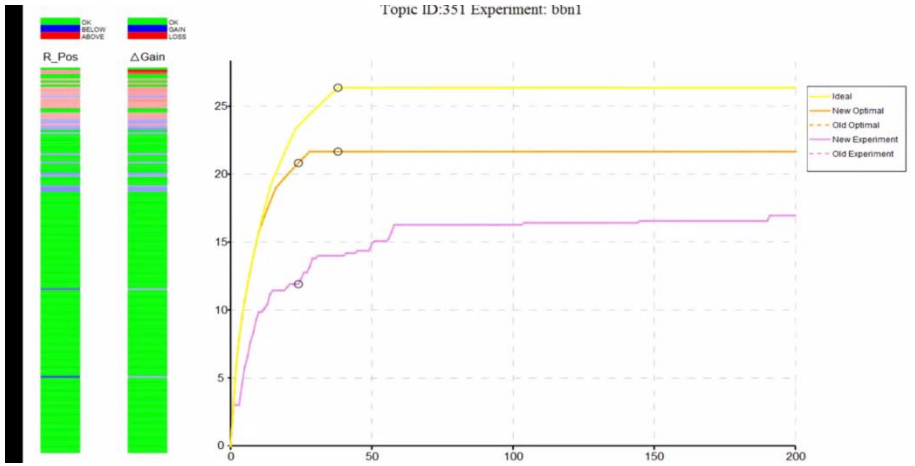
Novel visualization as well !





Demos

Tight integration



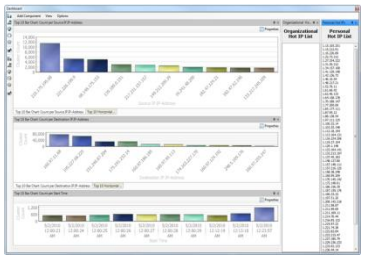
What if analysis

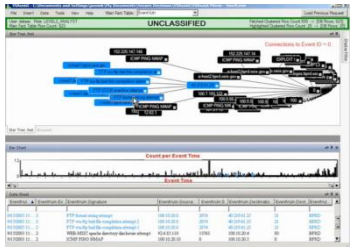
Moreover

- Engineers do not reinvent the wheel:
  - Look at commercial products
  - Look at similar projects

Back to PANOPTESEC - List of analyzed tools

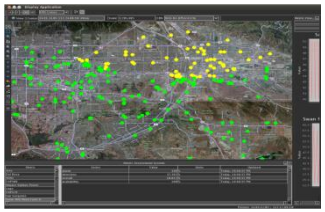
- VIAssist

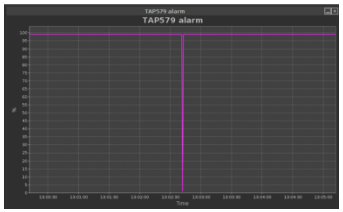




Commercial tool

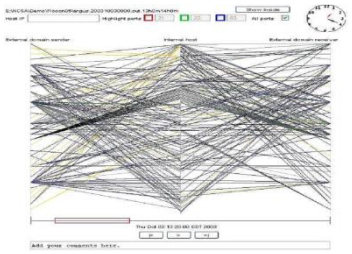
- CyberSAVE





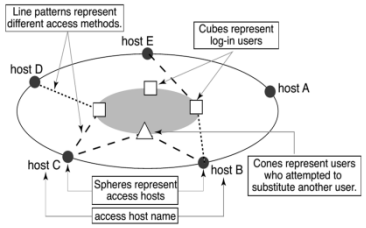
vizsec2013

- VisFlowConnect-IP



X. Yin, W. Yurcik, Y. Li, K. Lakkaraju, and C. Abad. VisFlowConnect: Providing security situational awareness by visualizing network traffic flows. In *23rd IEEE International Performance, Computing, and Communications Conference (IPCCC 2004)*, pages 601–607, Phoenix, AZ, 2004.

- Tudumi



T. Takada and H. Koike. Tudumi: Information visualization system for monitoring and auditing computer logs. In *Proceedings of the Sixth International Conference on Information Visualisation*, pages 570–576. IEEE, 2002.

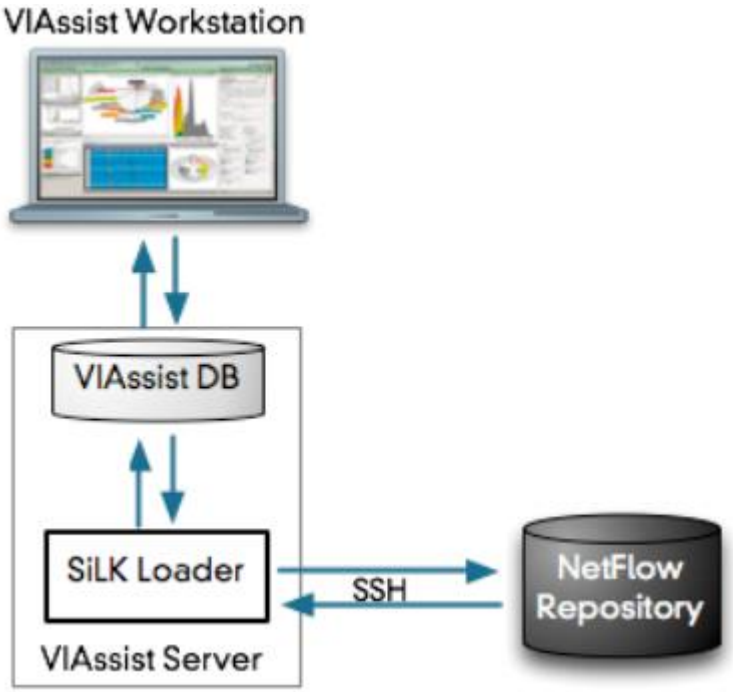
Summary

Tool	Attack model	Situation	Effects of attack	Risks	Automatic solutions	Semi-automatic solutions	Logs analysis
VIAssist	X	√	X	√	X	X	√
CyberSAVE	√	√	√	√	X	X	X
VisFlow Connect-IP	X	X	X	X	X	X	√
Tudumi	X	X	X	√	X	X	√

VIAssist
(commercial tool)

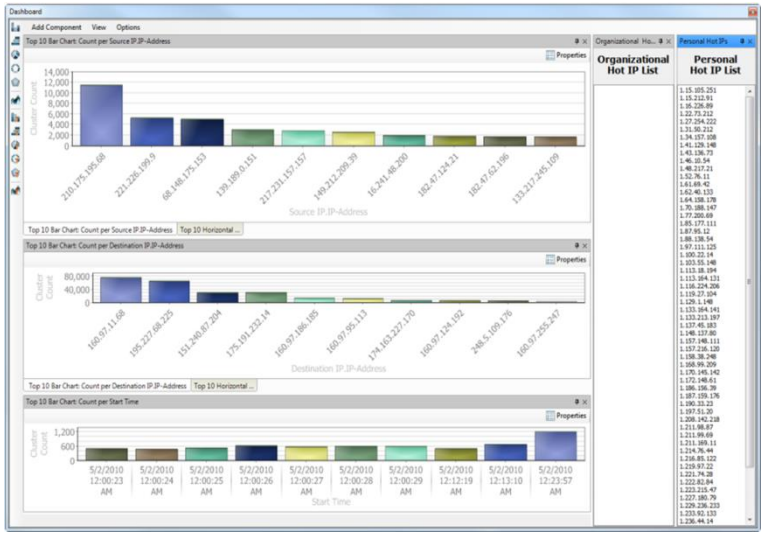
VIAssist

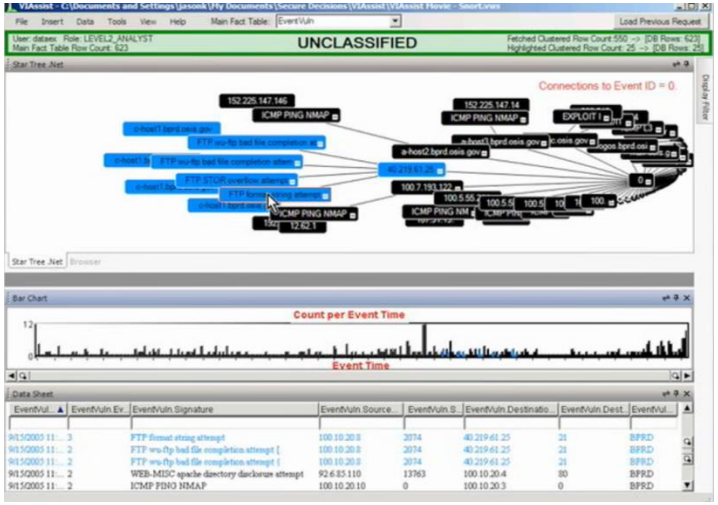
- pseudo real-time network data analyzer
- not an IDS (Intrusion detecting system) or sniffer
- displays data exported from a database that contains real-time information from an IDS or traffic analyzer



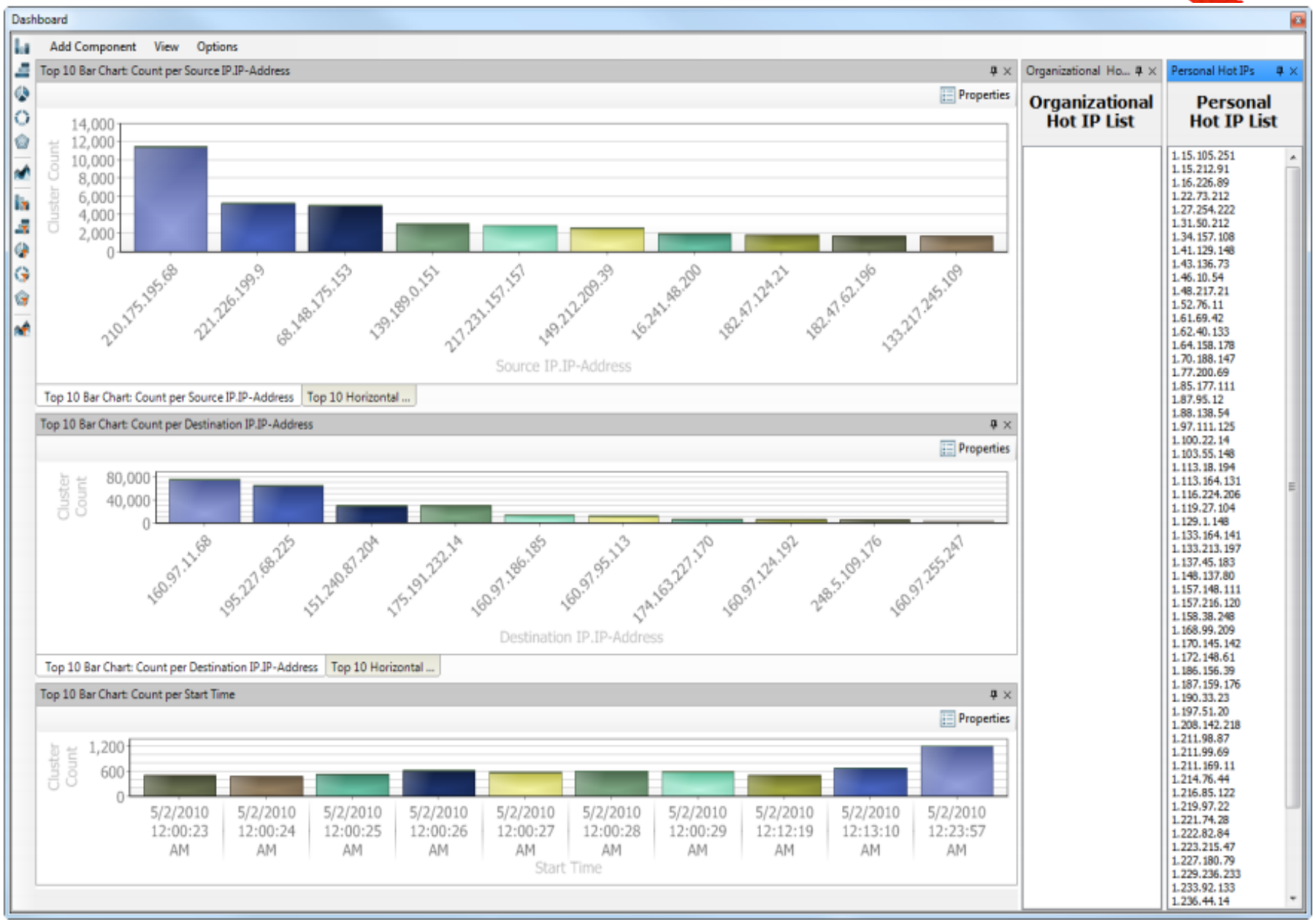
VIAssist - Situation

- the actual situation is shown by the usage of **charts** and **graphs**
- Selecting IPs as "hot IPs", to highlight them
- more specific analysis with a graph on suspicious IP, showing all the host that communicates with this suspicious IP

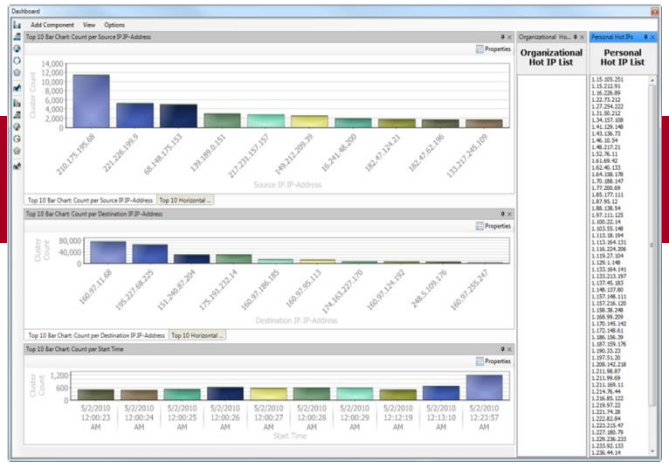




VIAssist – Situation: IP analysis



VIAssist - Situation



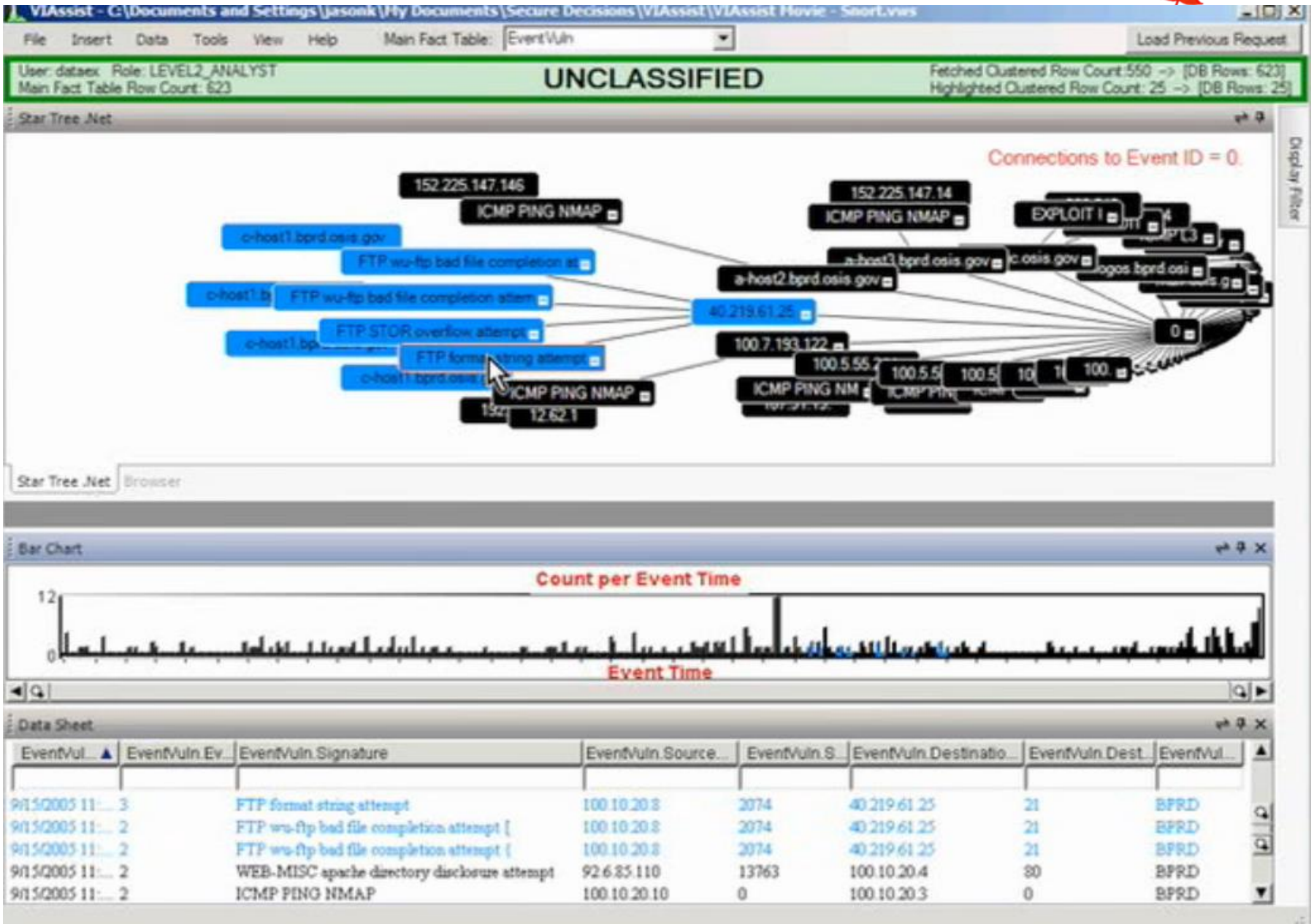
Description

- In the right panels, we find the IP list that we want to highlight (hot IPs);

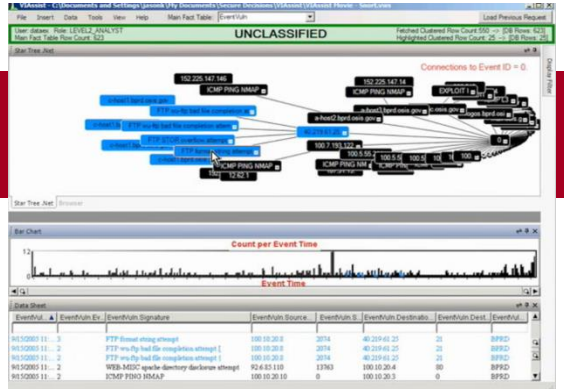
- On the left we have three charts having on the x-axis:
  - 1) source IP address
  - 2) destination IP address
  - 3) time intervals

  On the y-axis they have the number of connections for a specific IP address or in a specific time interval

VIAssist – Situation : Network of IP traffic



VIAssist - Situation



Description

Top) We can also have a visualization in which we can see all the connections between a specific (maybe suspicious) node with other nodes in the network (on the top).

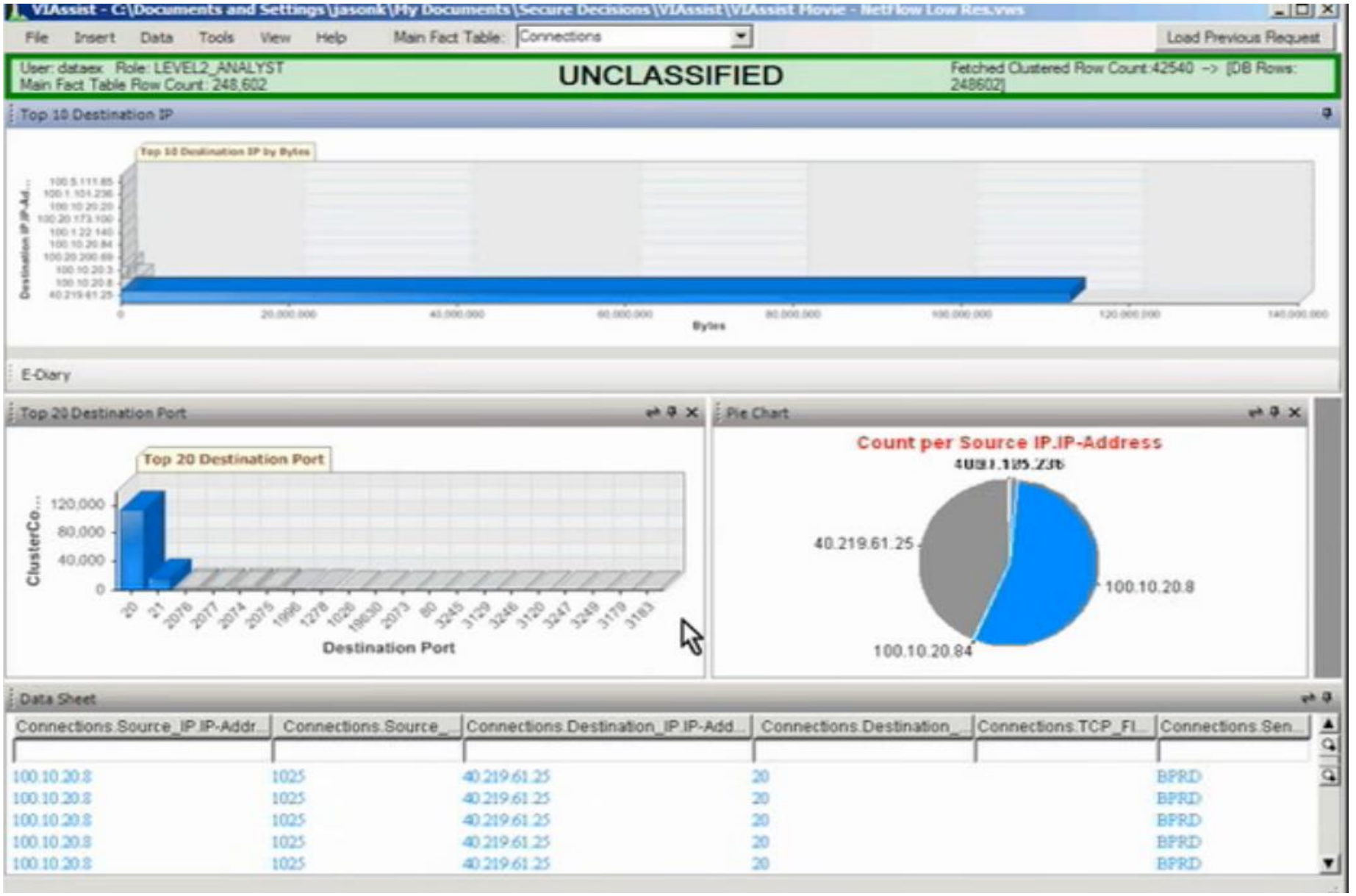
Middle) we have highlighted in blue the traffic (FTP traffic for instance) that was originating some suspicious. Moreover, here we can see when every piece of traffic was exchanged between two nodes.

Bottom) we have the textual version of the top and middle parties explaining all the characteristics of the traffic

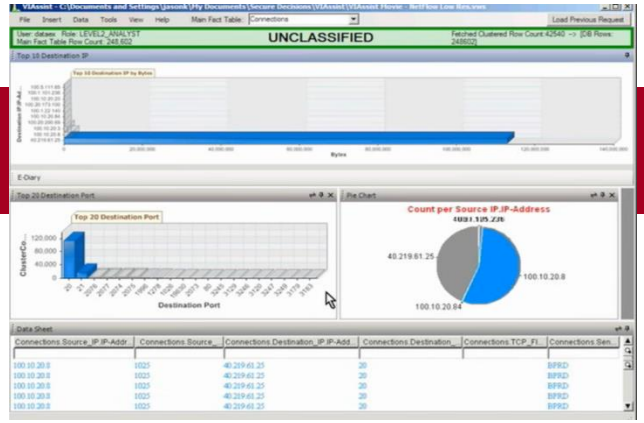
VIAssist - Risks

- the analysis of the risks is done by viewing and inspecting the network traffic
- for a specific host we can :
  - see the amount of bytes received
  - see the ports used to communicate
  - verify if there is one or more suspicious hosts that are overloading the traffic
  - if we are protecting a "local" network we have also a geographic visualization that permits to see if there are external (not desirable) communication in act

VIAssist - Risks



VIAssist - Risks



Description

Top) Chart that describe the IP addresses with the most quantity of bytes received

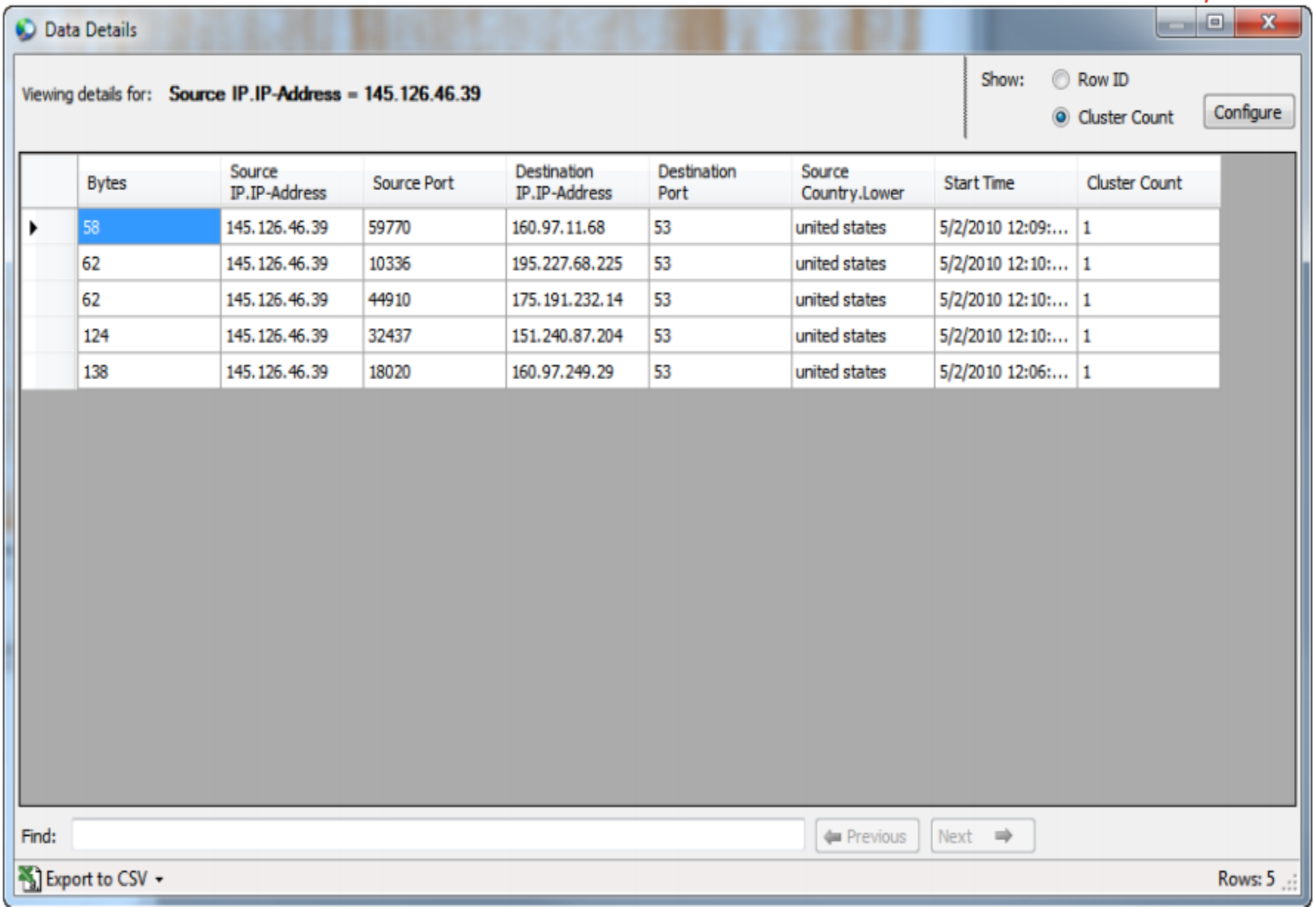
Middle-left) Ports used through which was transferred the quantity of bytes indicated on the top chart

Middle-right) Cake chart indicating the source partners of the communications.

VIAssist - Logs analysis

- to analyze the logs we have many type of charts that help us to understand the following properties of the network traffic :
  - type
  - port
  - amount
  - source/destination IP
  - trends (with the creation of reports)

VIAssist - Logs analysis example



Bytes	Source IP.IP-Address	Source Port	Destination IP.IP-Address	Destination Port	Source Country.Lower	Start Time	Cluster Count
58	145.126.46.39	59770	160.97.11.68	53	united states	5/2/2010 12:09:...	1
62	145.126.46.39	10336	195.227.68.225	53	united states	5/2/2010 12:10:...	1
62	145.126.46.39	44910	175.191.232.14	53	united states	5/2/2010 12:10:...	1
124	145.126.46.39	32437	151.240.87.204	53	united states	5/2/2010 12:10:...	1
138	145.126.46.39	18020	160.97.249.29	53	united states	5/2/2010 12:06:...	1

CyberSAVE
(research tool)

CyberSAVE

- Cyber Situational Awareness for visualization
- visualization of trust in the nodes of a network to allow a user to make critical decisions
- the trust is computed through a mathematical model

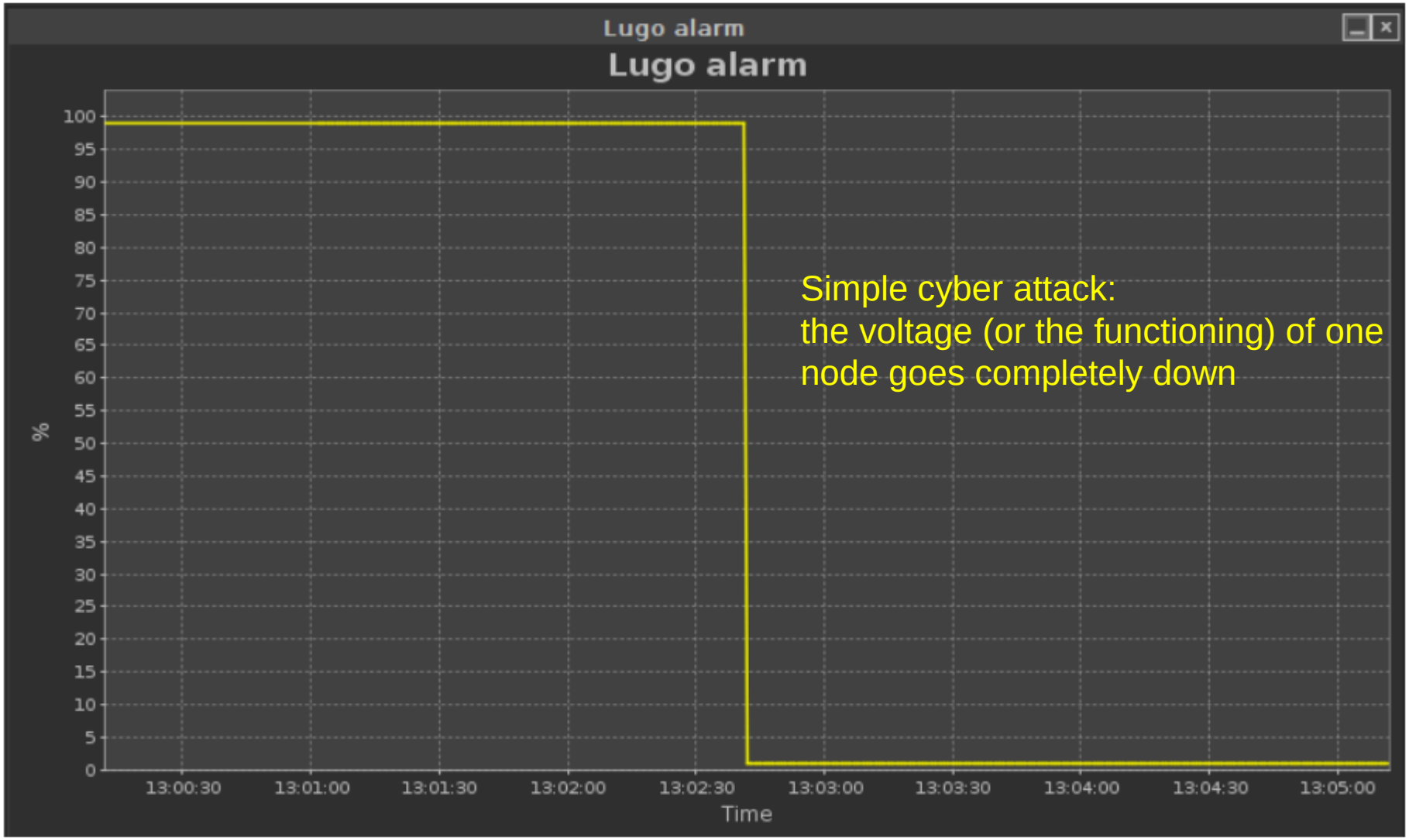
CyberSAVE - Attack model

- the modeling of an attack is based on the standard response of the system to a certain type of attack

- Type of attack :
  - physical attack
  - known malware attack
  - simple cyber attack
  - advanced cyber attack
  - advanced collusion attack

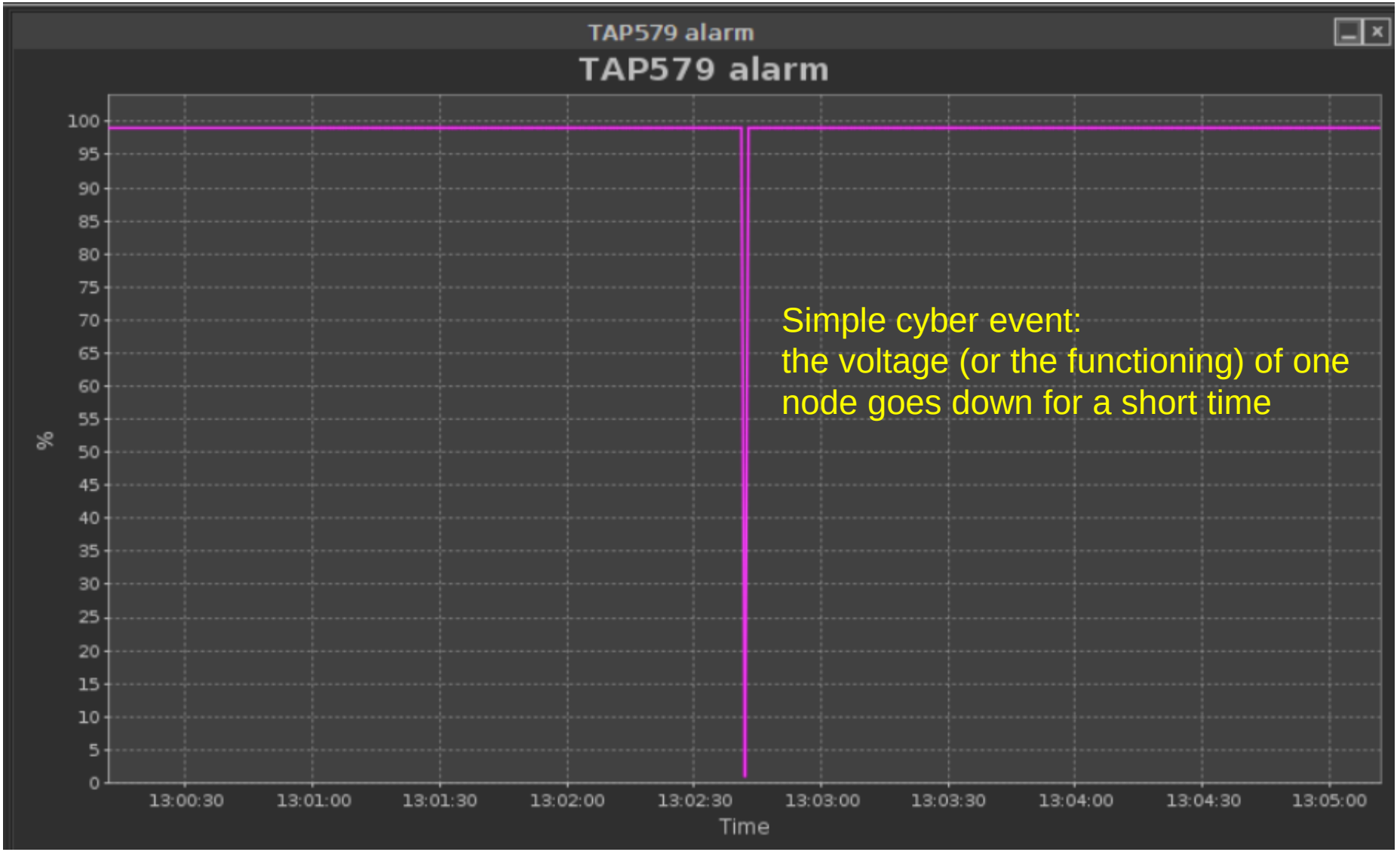
Protection vs Attack	Sensor	+Firewall	+Cyber Trust	+Predictability	+Visualization
Physical Attack (PA)	✔	✔	✔	✔	✔
Simple Cyber Attack (SCA)		✔	✔	✔	✔
Intermediate Cyber Attack			✔	✔	✔
Advanced Cyber Attack				✔	✔
Advanced Collusion Attack					✔

CyberSAVE - Attack model



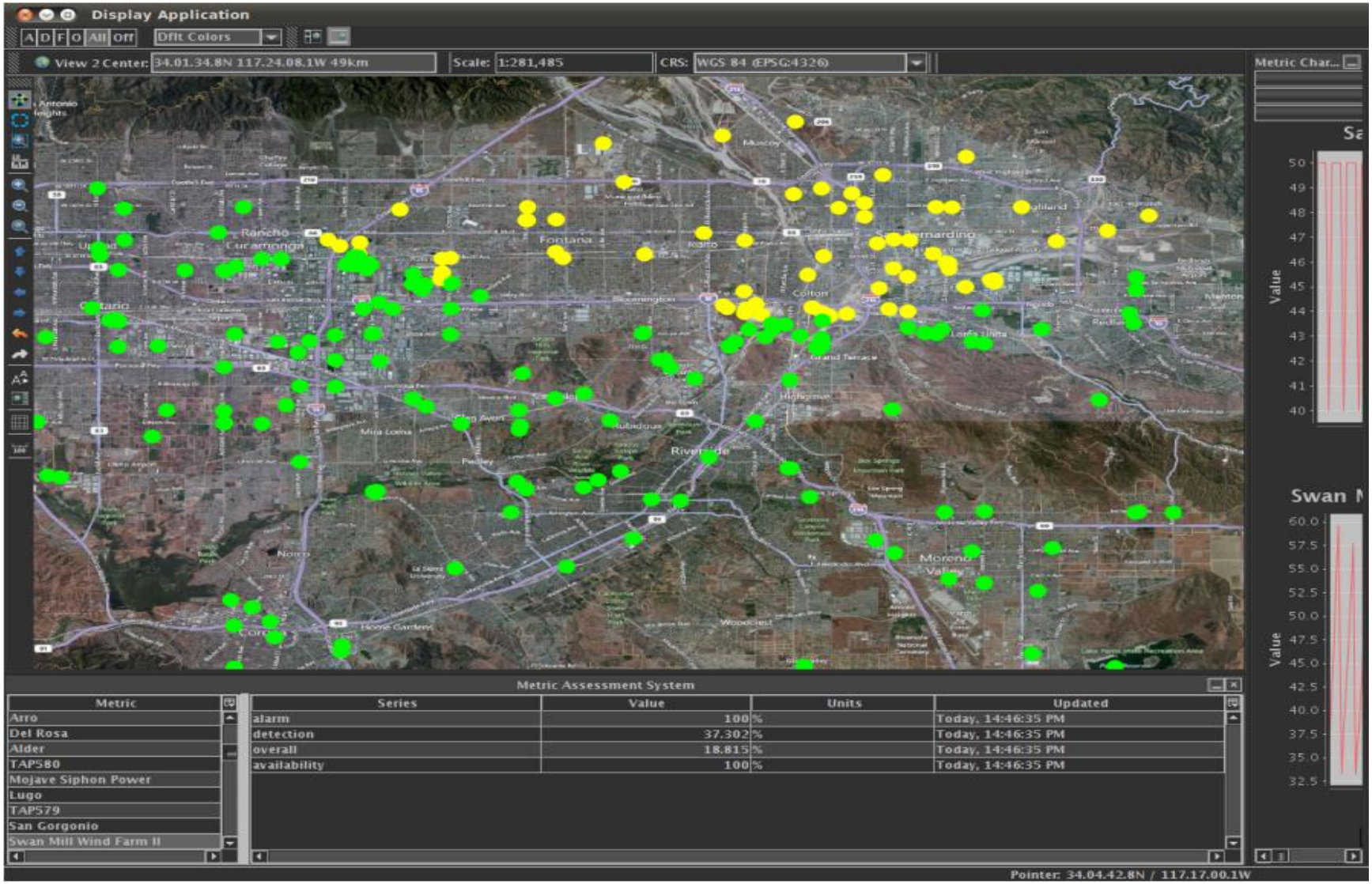
Example of Simple cyber attack

CyberSAVE – Cyber event



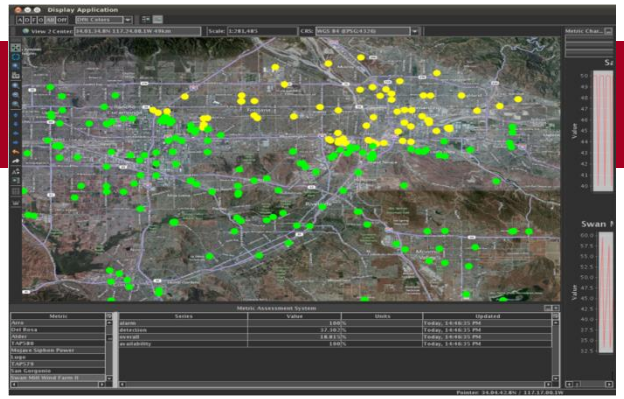
Example of One-time cyber event

CyberSAVE - Attack model



Example of Geographic attack result

CyberSAVE - Attack model



Description

In the geographic attack, we have a map and points of different color (green, yellow) depending if the node was attacked.

The operator can analyze the metrics by the bottom part of the visualization (textual part) and by the right part that explains through charts the type of attack that was done.

This part is comprehensive of the prevention part because the operator can put offline the nearby nodes to isolate the attack

CyberSAVE - Situation / Risks

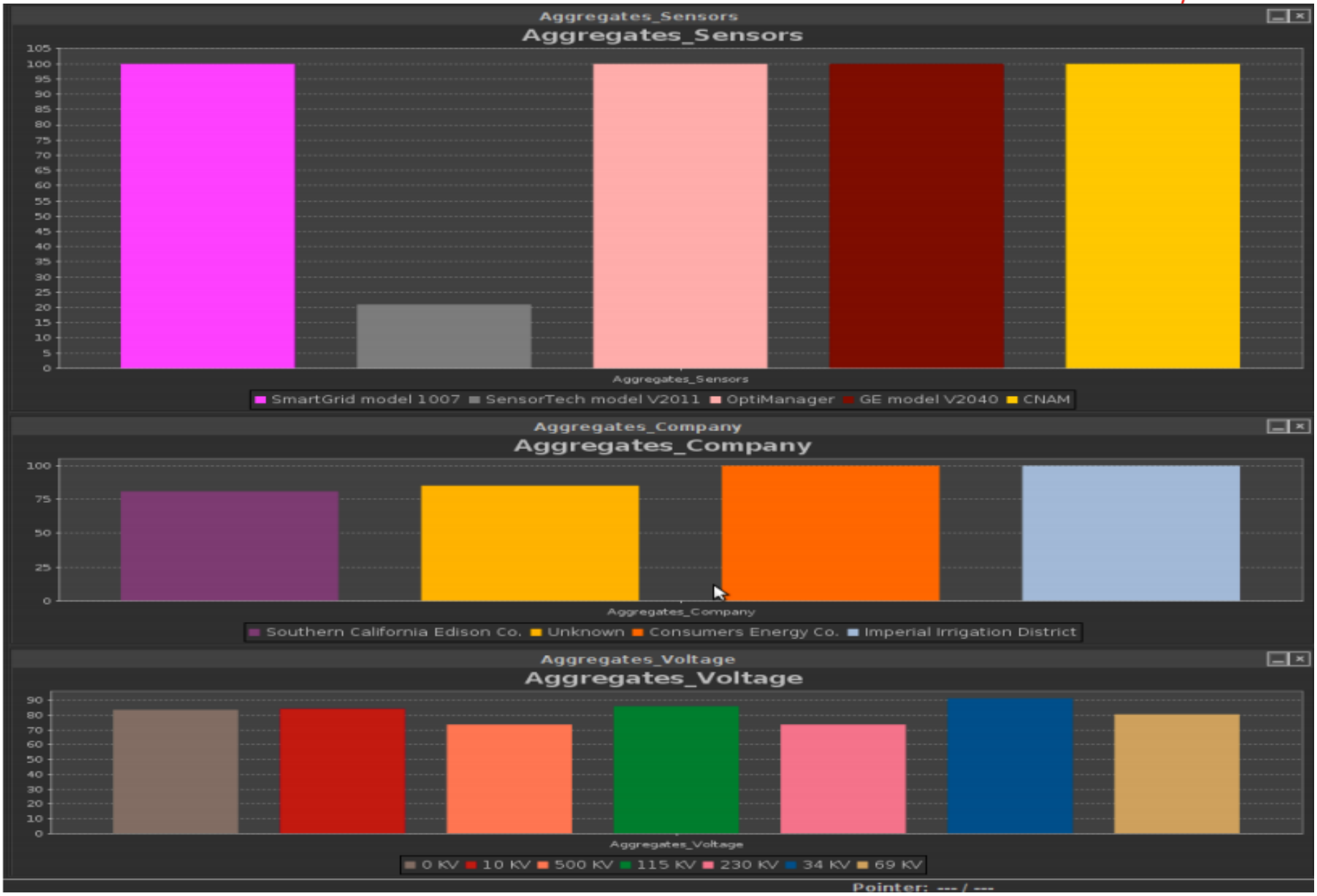
Data aggregation :

- consider trust data of nodes that share certain common characteristics
- provide awareness of the situation, potential risks and threats not obvious otherwise

Examples of aggregation : geographic, network parameters, equipment manufacturer, software environment, trust type

- if the operator discover not acceptable values, it can do a deep analysis of the nodes or begin some actions

CyberSAVE - Situation / Risks



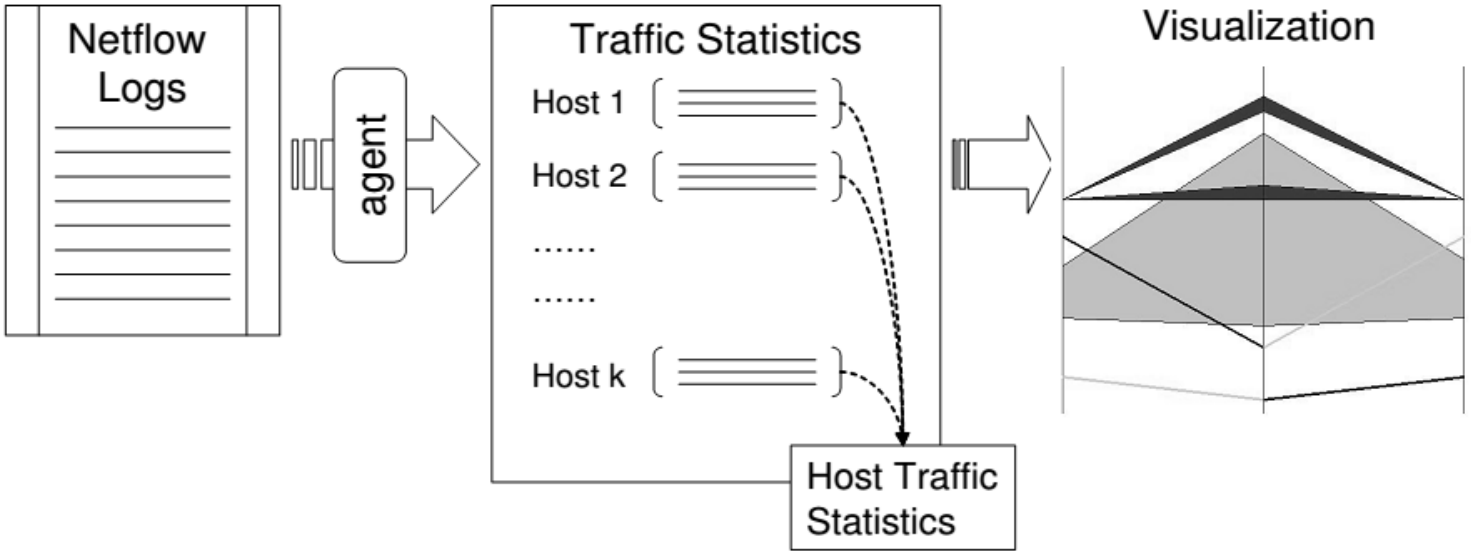
VisFlowConnect-IP
(research tool)

VisFlowConnect-IP

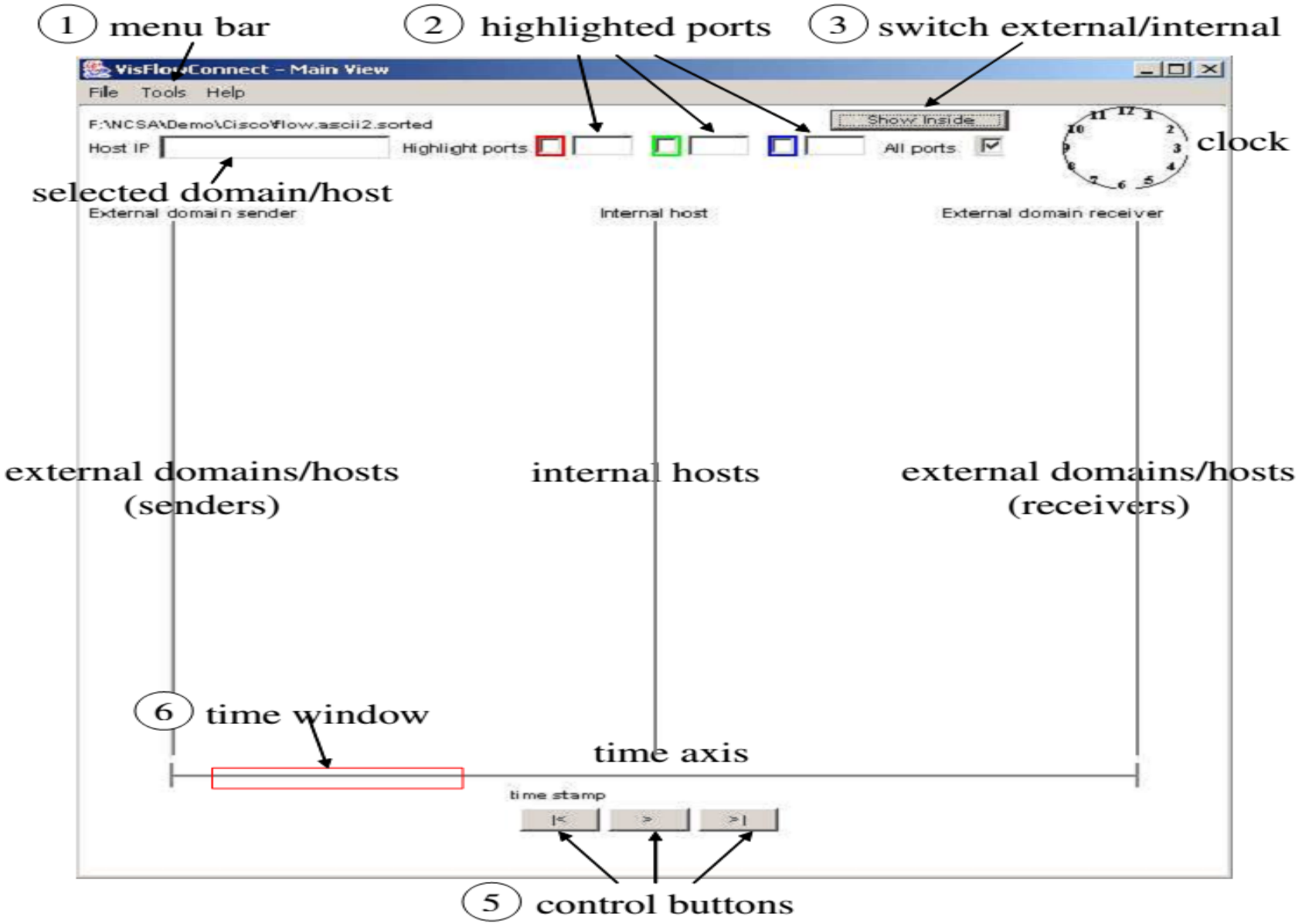
- flow visualization tool
- allows operators to detect and investigate anomalous internal and external network traffic
- model : parallel coordinates in which nodes = hosts and traffic = flow on edges (as lines between nodes)
- graph animation over time can reveal some trends
- features :
  - animations to visualize network traffic
  - multi-level views of network traffic including an overview and drill-down views to query for details
  - filtering capabilities to remove known legitimate traffic so as to focus on potential security events

VisFlowConnect-IP - Description

- 3 main components :
  - input agent that extracts NetFlow records (containing IP source-destination, ports, bytes, timestamps and protocol)
  - NetFlow analyzer that processes raw data
  - visualizer that converts statistics into graphical animation



VisFlowConnect-IP - Logs analysis



VisFlowConnect-IP - Logs analysis

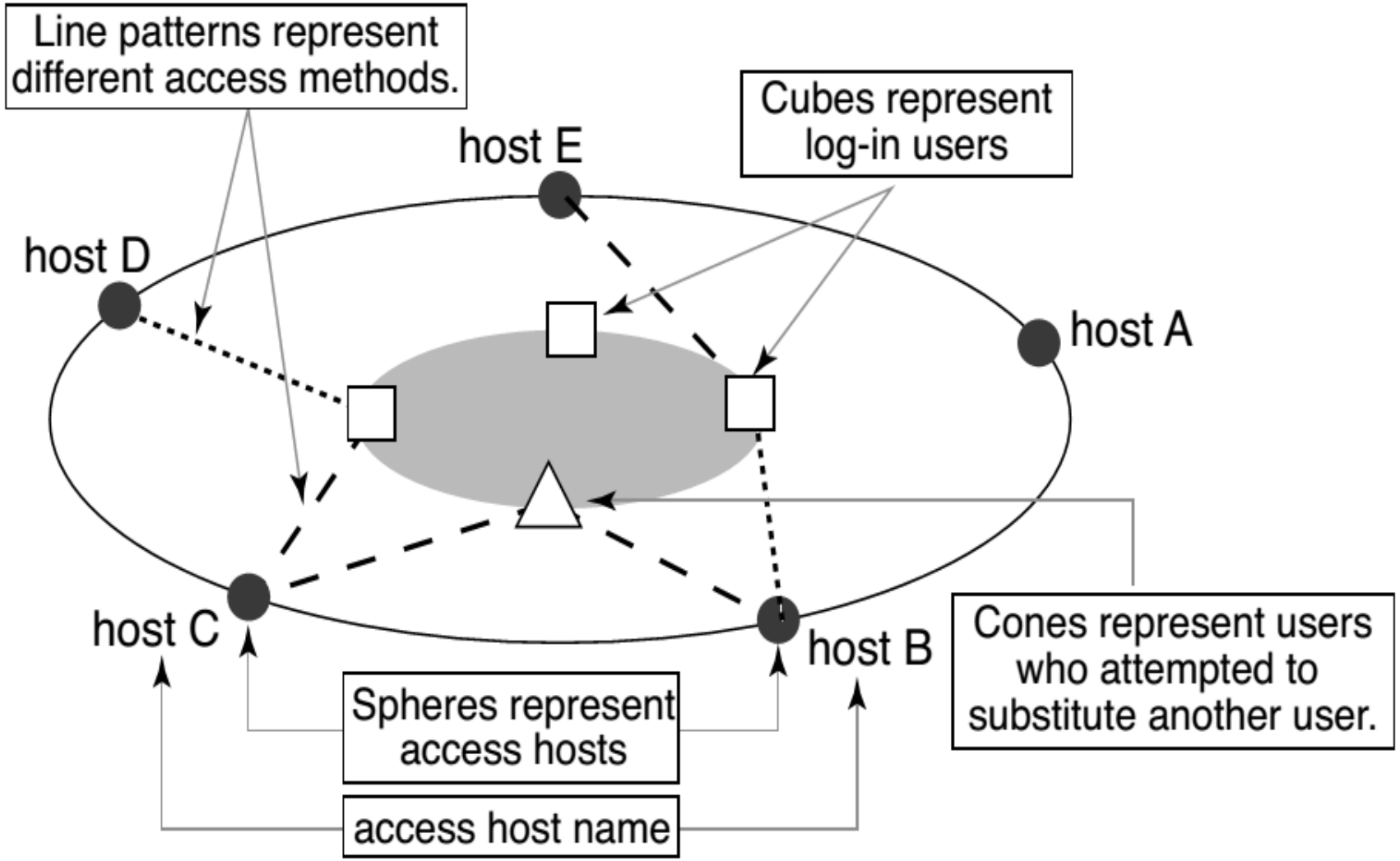
Tudumi
(research tool)

Tudumi - Description

- analysis of computer logs stored in a server accessed by many users
- client/server model in which the client can monitor and audit more than one server
- computer logs = huge amounts of textual data
- functions :
  - info visualization
  - log summarization
  - reflect security rules into the visulization method

- 3 kinds of user activities : accessing the server, logging into the server and substituting a user to another user

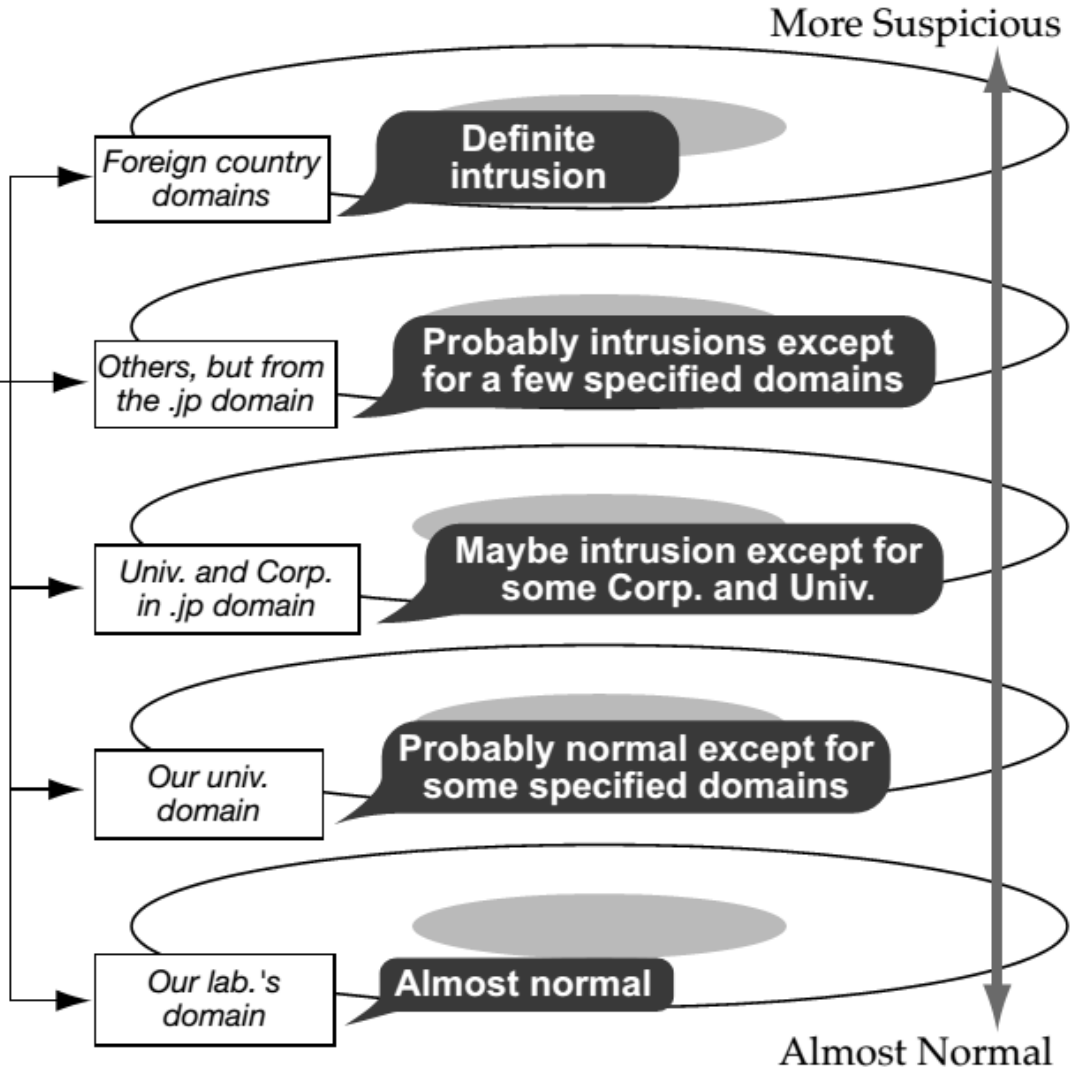
Tudumi - Info representation



Tudumi - Risks

Define the classification rules based on the probability of the emregence of each event and assign them to each layer

Intrusive behaviors are extracted visually

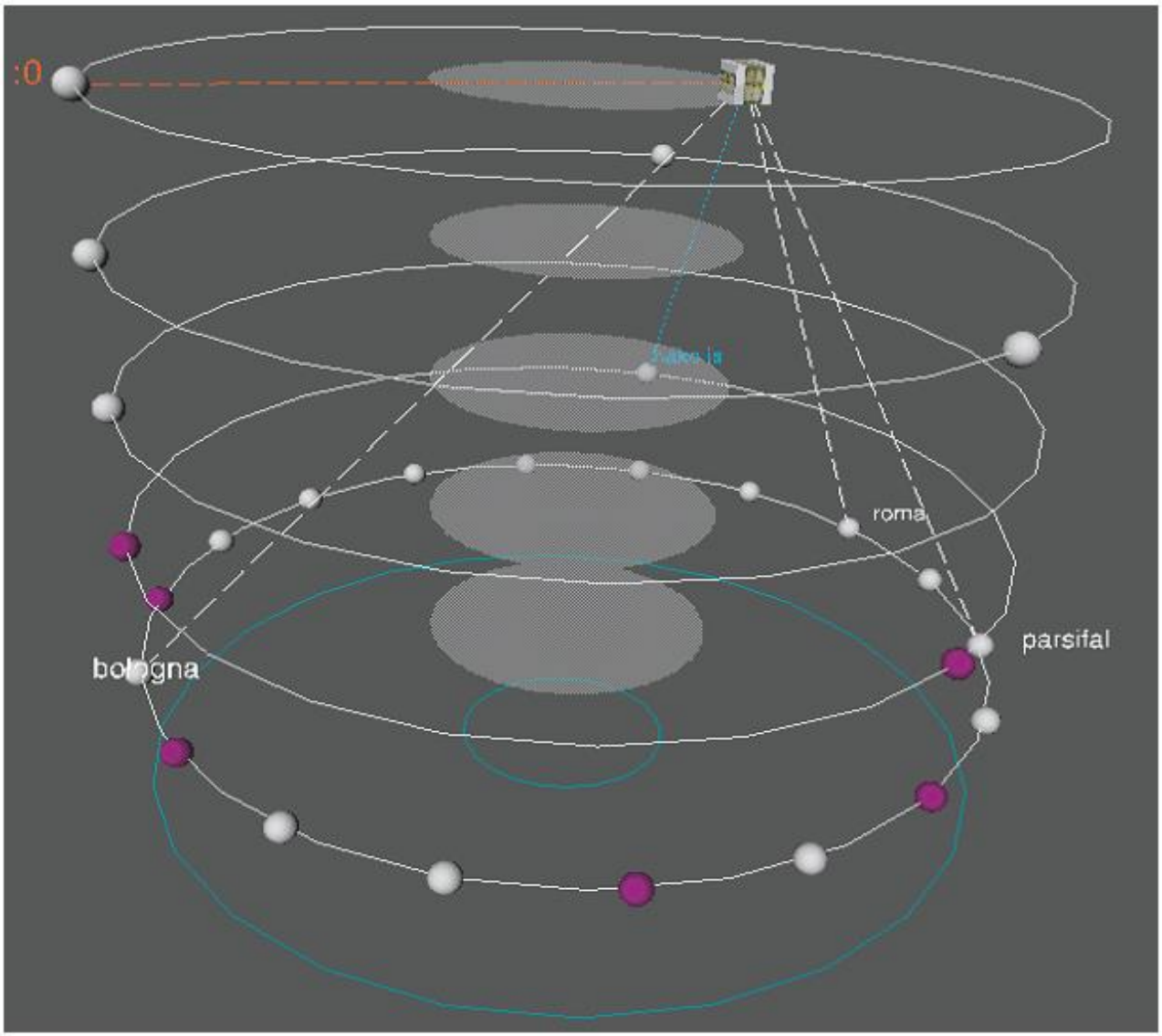


Tudumi - Risks

- It is possible to define many rules regarding accesses and user log-in to hosts
- Through an interface made by layered concentric disks, the informations about possible malicious activities are highlighted from the most suspicious type of activity to the less suspicious one.
- The disks are divided into two groups :
  - the bottom disk : user substitution information
  - other disks : network access + user login information

- We can see the risks on the network depending from the rules that we have specified.
- Example 1 (see next slide) :

Tudumi - Risks

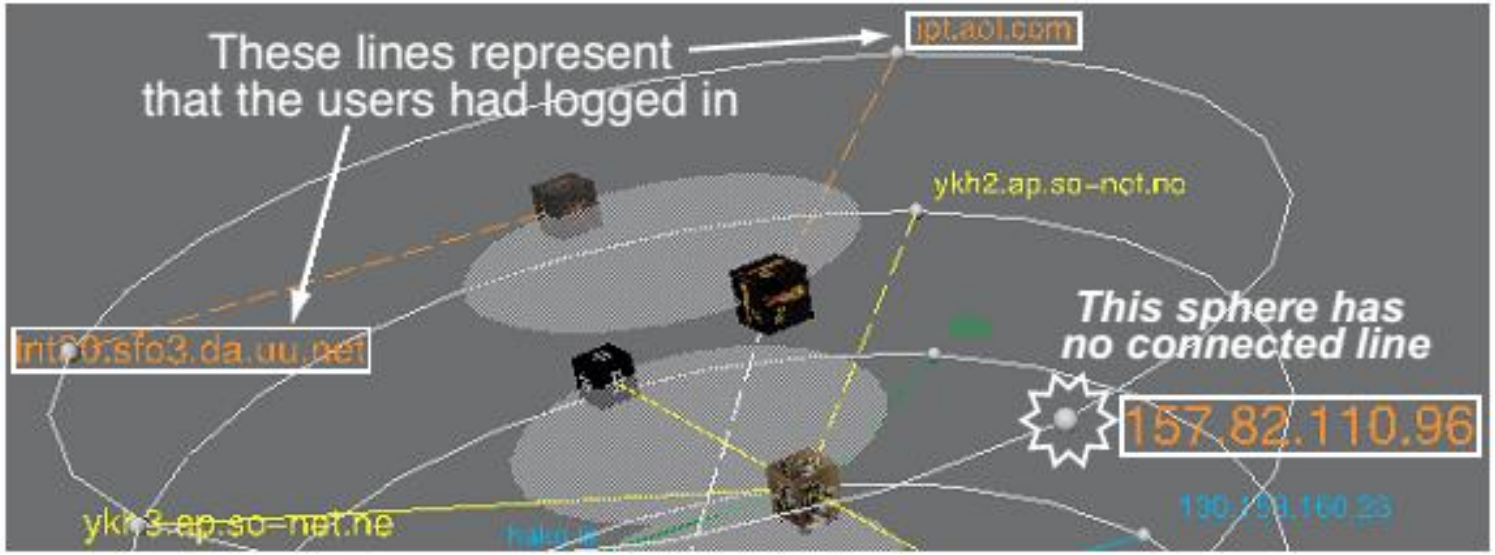


Example 1
If we have declared accesses from foreign domains as more suspicious and if this type of communication happen, then we are able to see this type of risk (first of other risks because it will be on the upper disk)

Tudumi - Risks

Example 2

The sphere has no connected line in the figure and this represents the existence of an anomalous access (someone accessed the monitored host but she/he could not login)

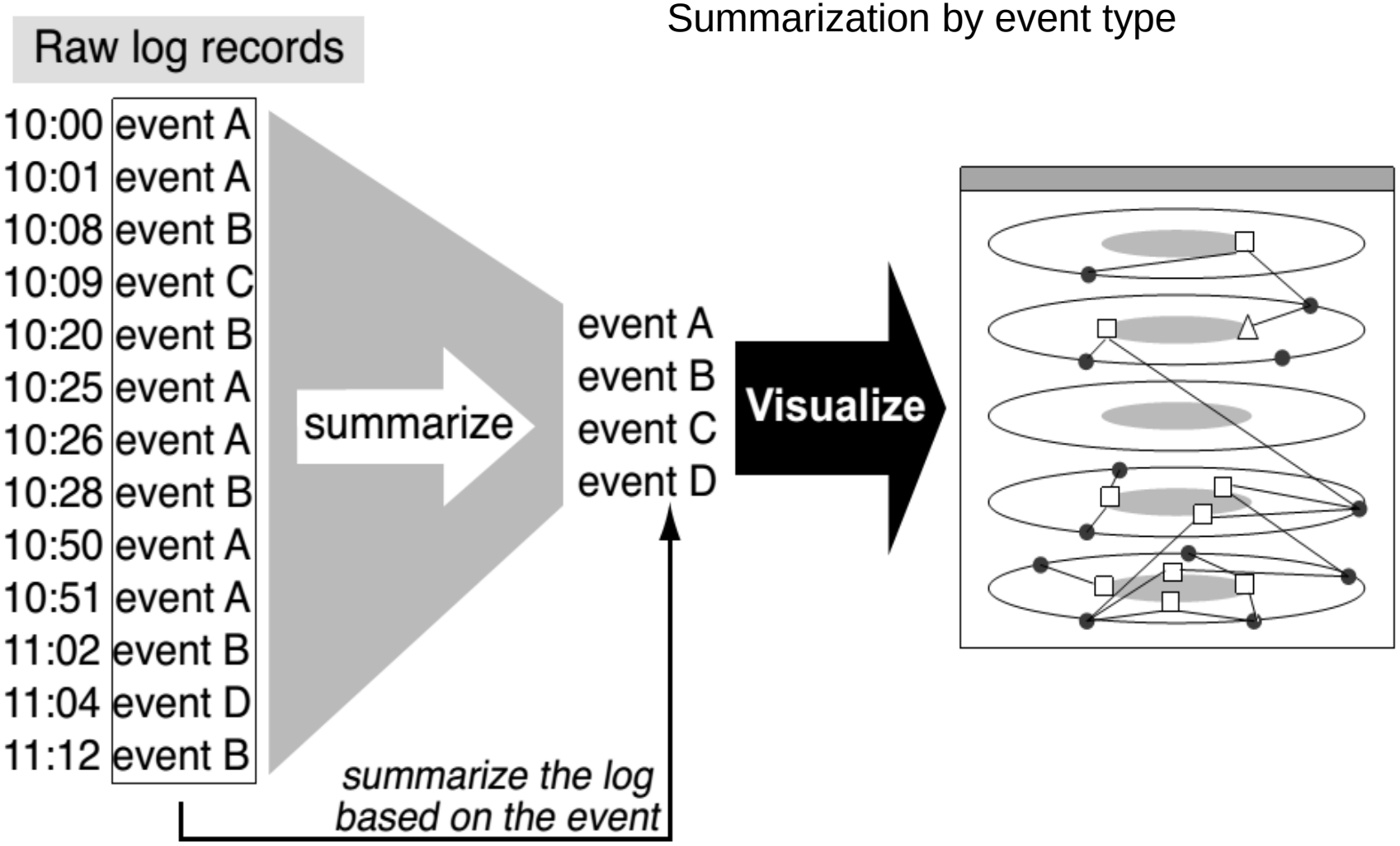


Tudumi - Logs analysis

- The logs analysis is based on the log summarization and on the type of summarization we do because the textual log data is very huge
- This activity is useful in order to eliminate the excess messages (as we can see in the next slide)
- Obviously, the logs (after they are summarized) are visualized into the layered visualization of before and we can click on a specific host, to get information about the type of the connection

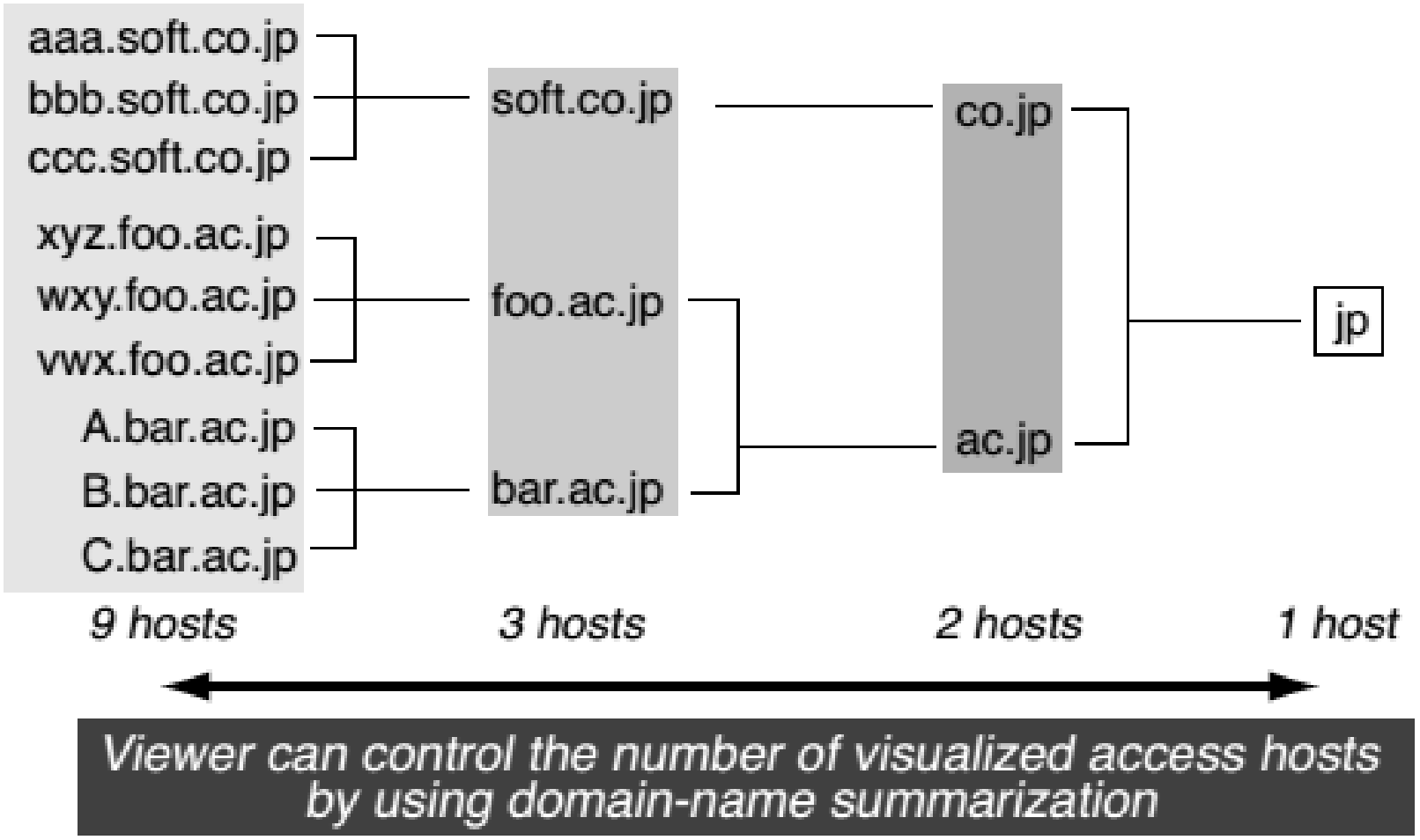
Tudumi - Logs analysis

Summarization by event type



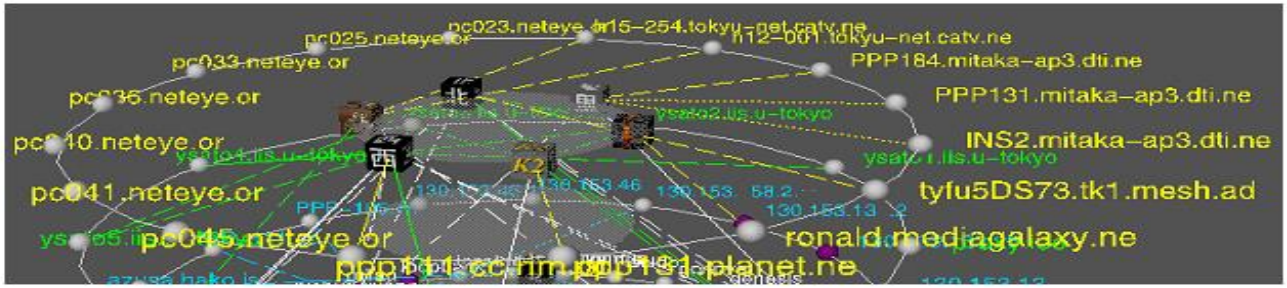
Tudumi - Logs analysis

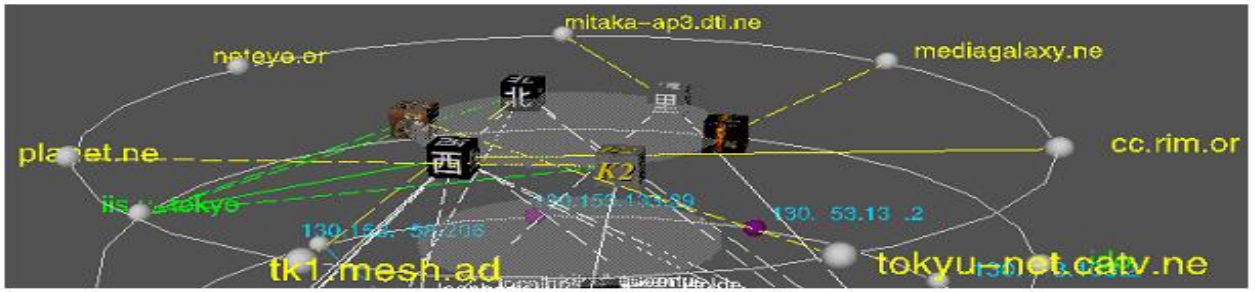
Summarization by domain name



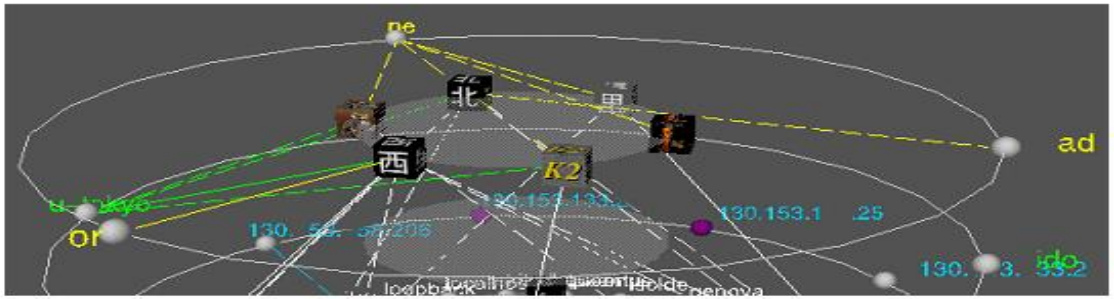
Tudumi - Logs analysis

Actual data representation





Summarized representation



It is easy to recognize the fact.

There are the accesses from 3 sub domains.

Mockup Design for Panoptesec

Models (work in progress…)

- We propose three models:

  1. Single-property analysis model
  2. Proactive-Reactive model
  3. Mixed analysis model

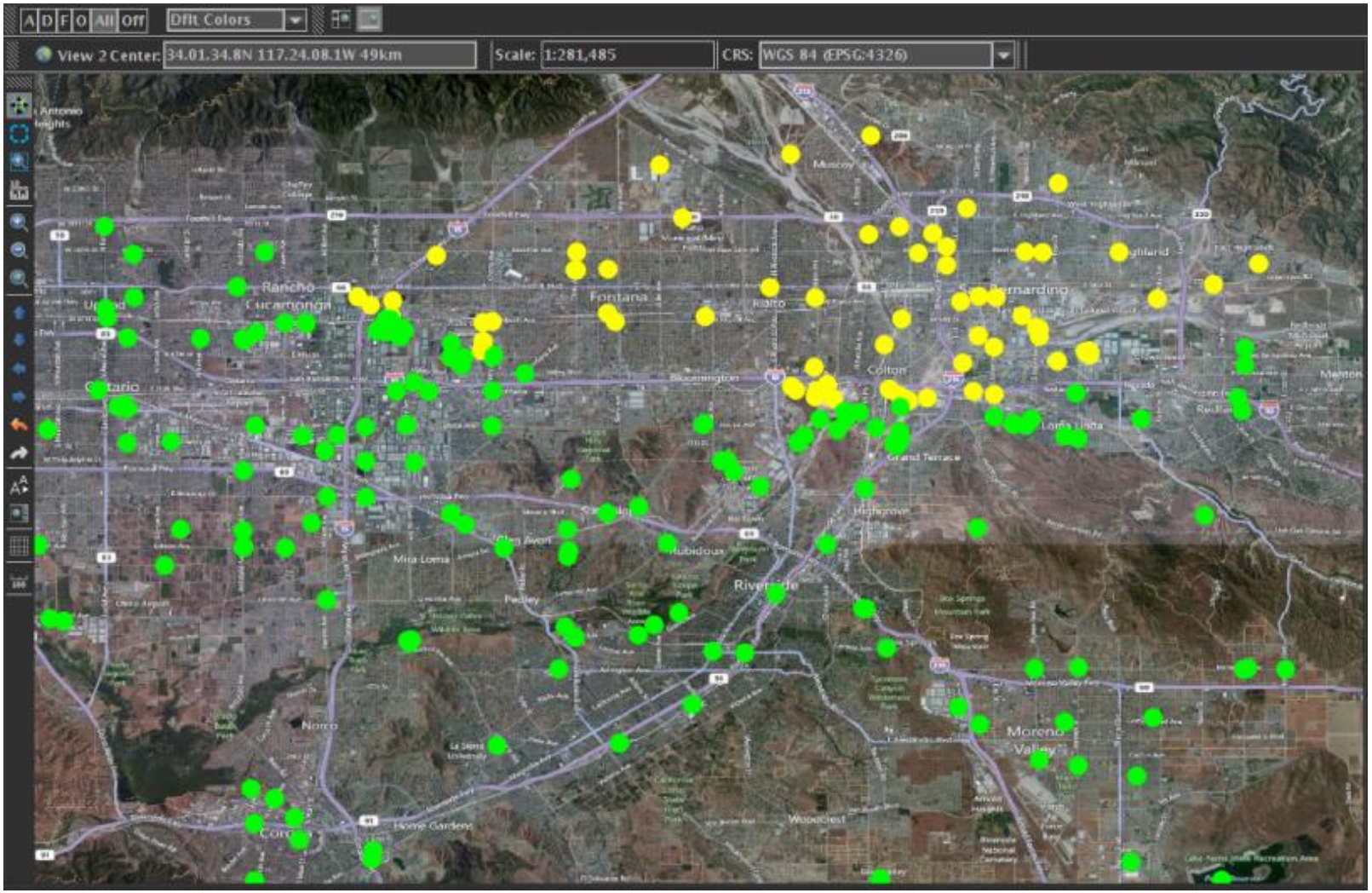
Single-property analysis model

In this model, we have one module for each property that we want to analyze :

- attack model
- situation
- effects of attack
- risks
- logs analysis

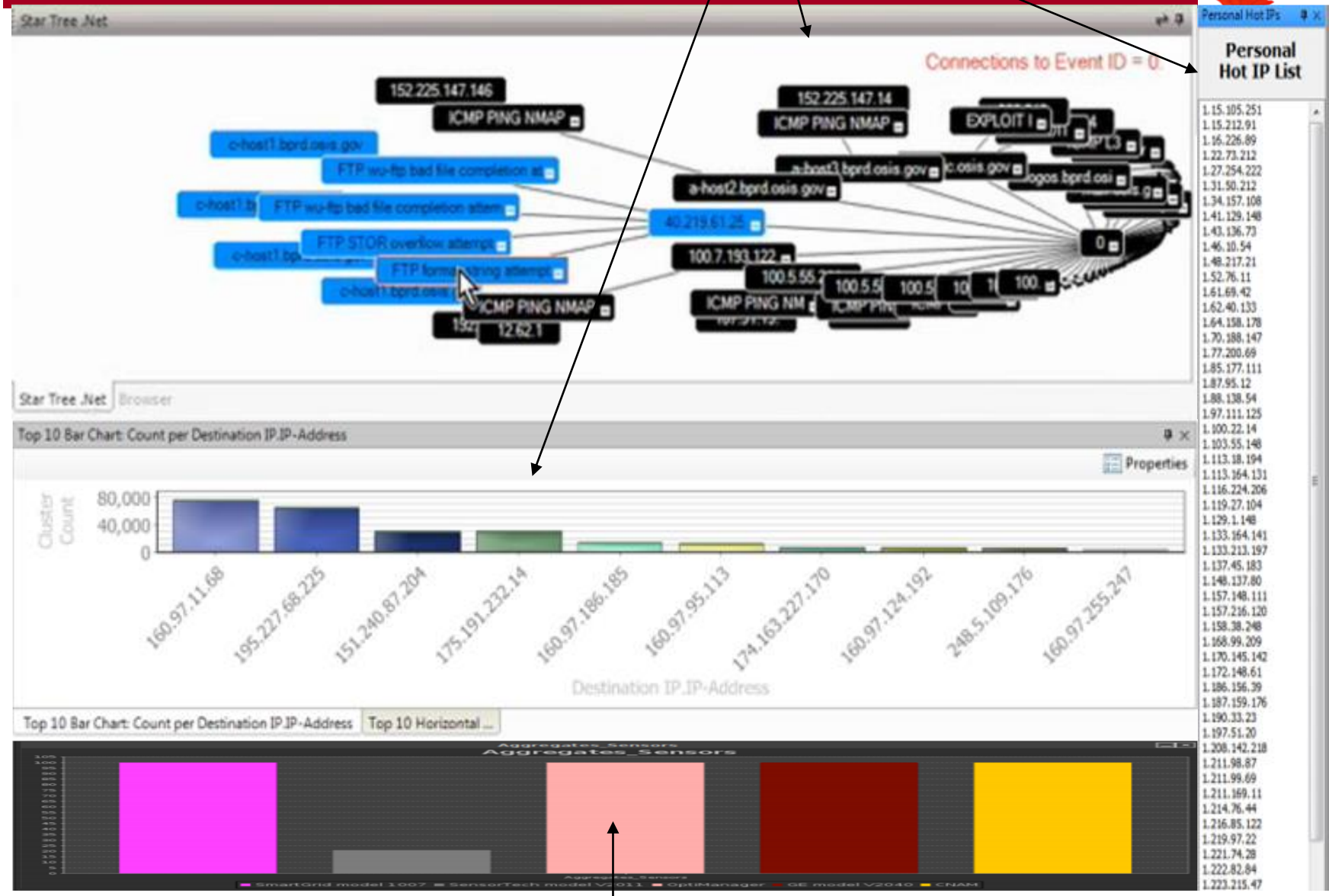
Attack model

CyberSAVE - Research tool



Situation

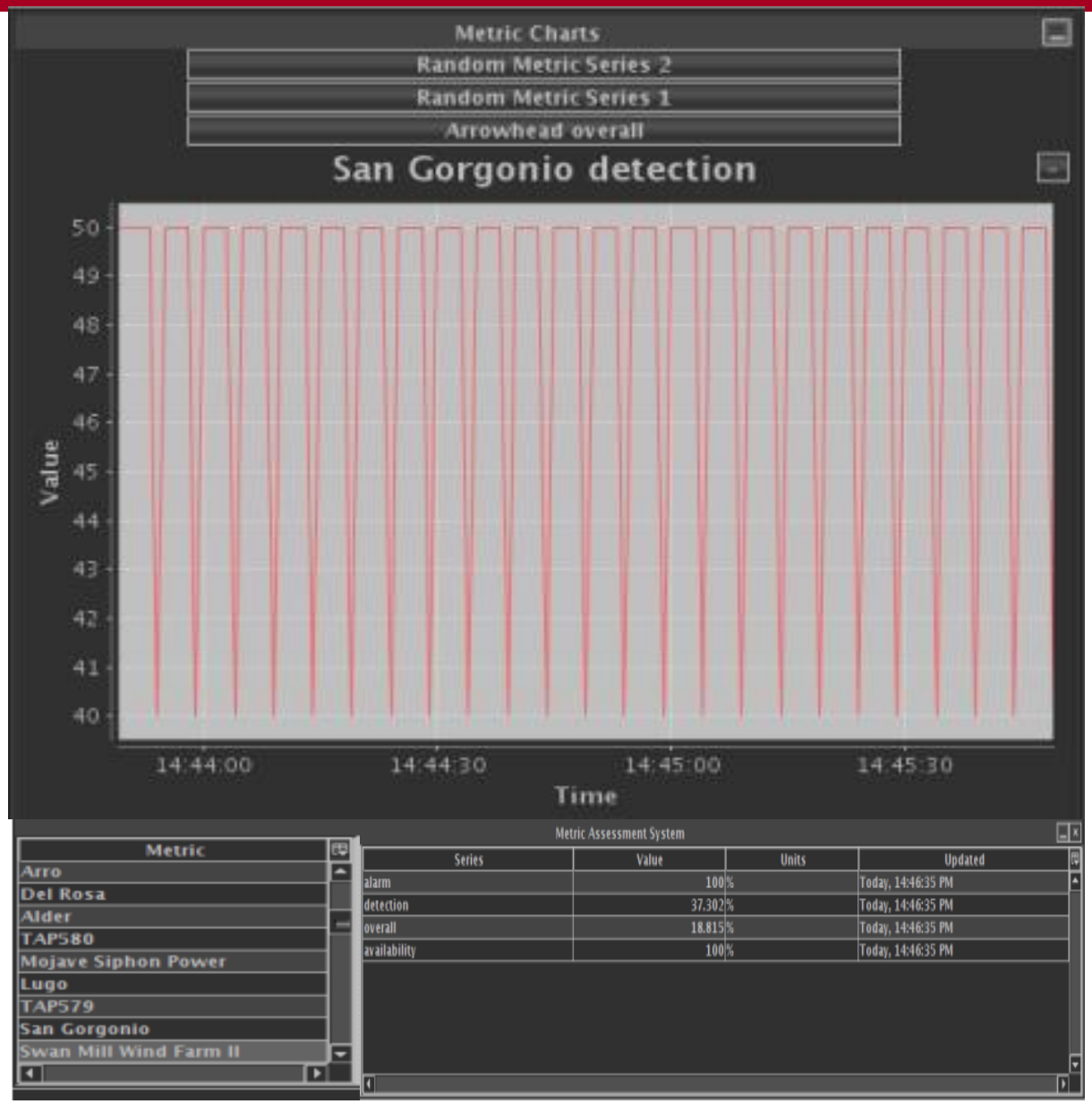
VIAssist - Commercial tool



CyberSAVE - Research tool

Effects of the attack

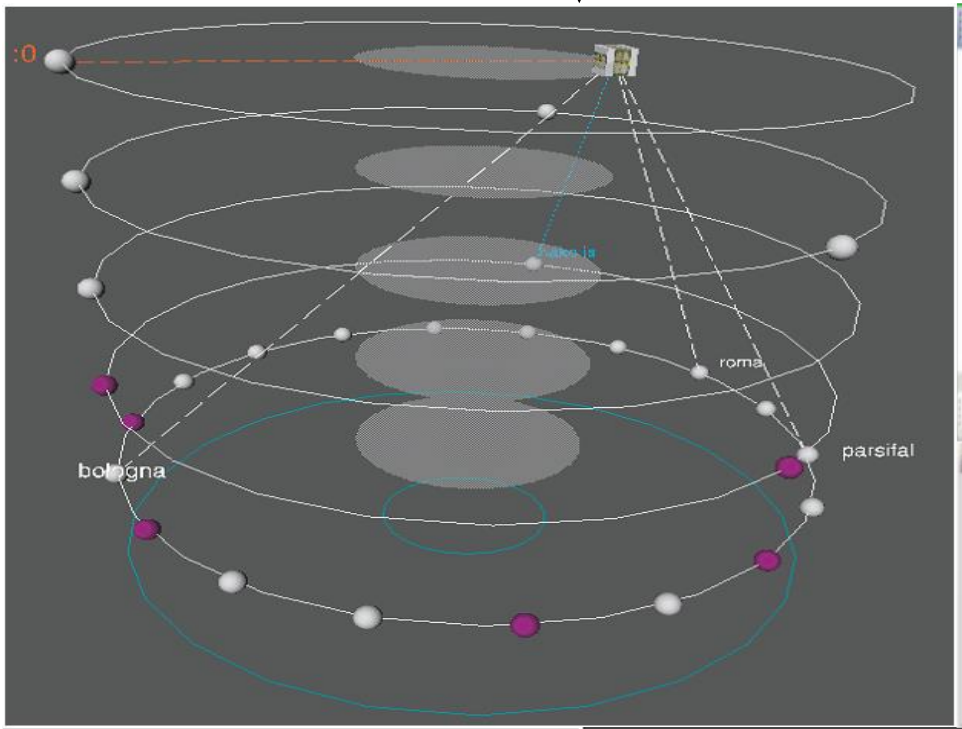
CyberSAVE - Research tool

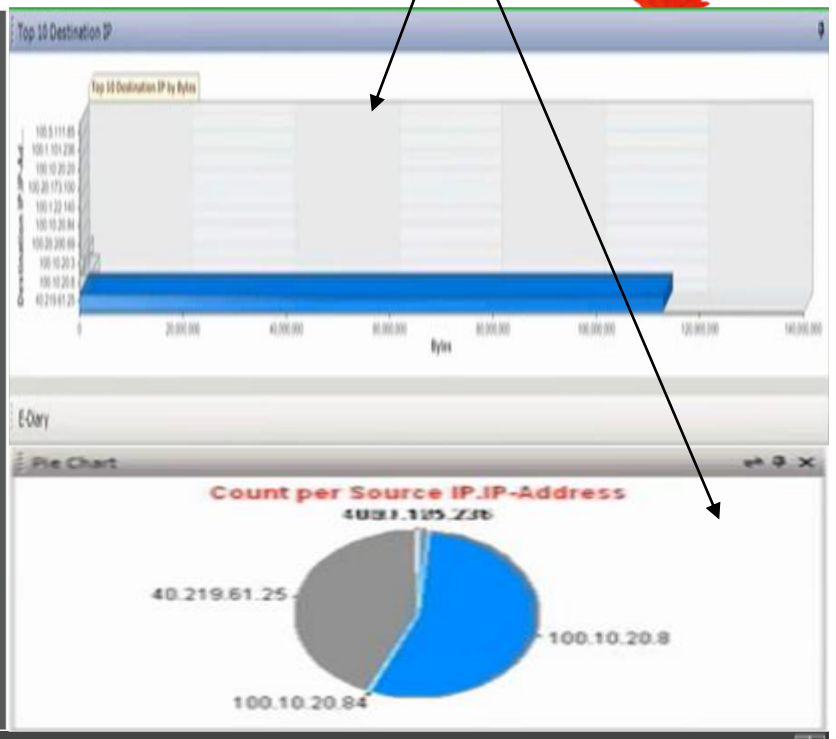


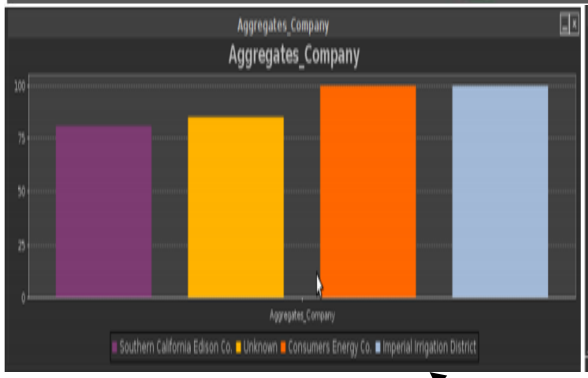
Risks

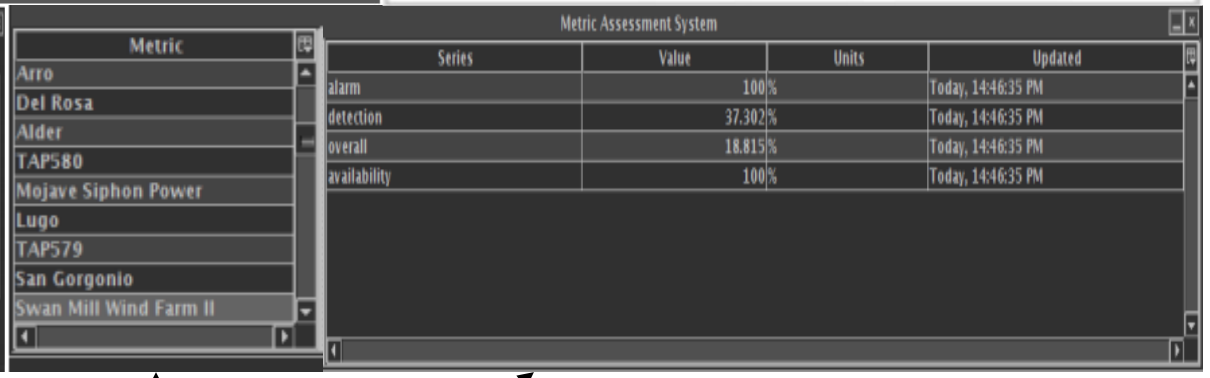
Tudumi - Research tool

VIAssist - Commercial tool





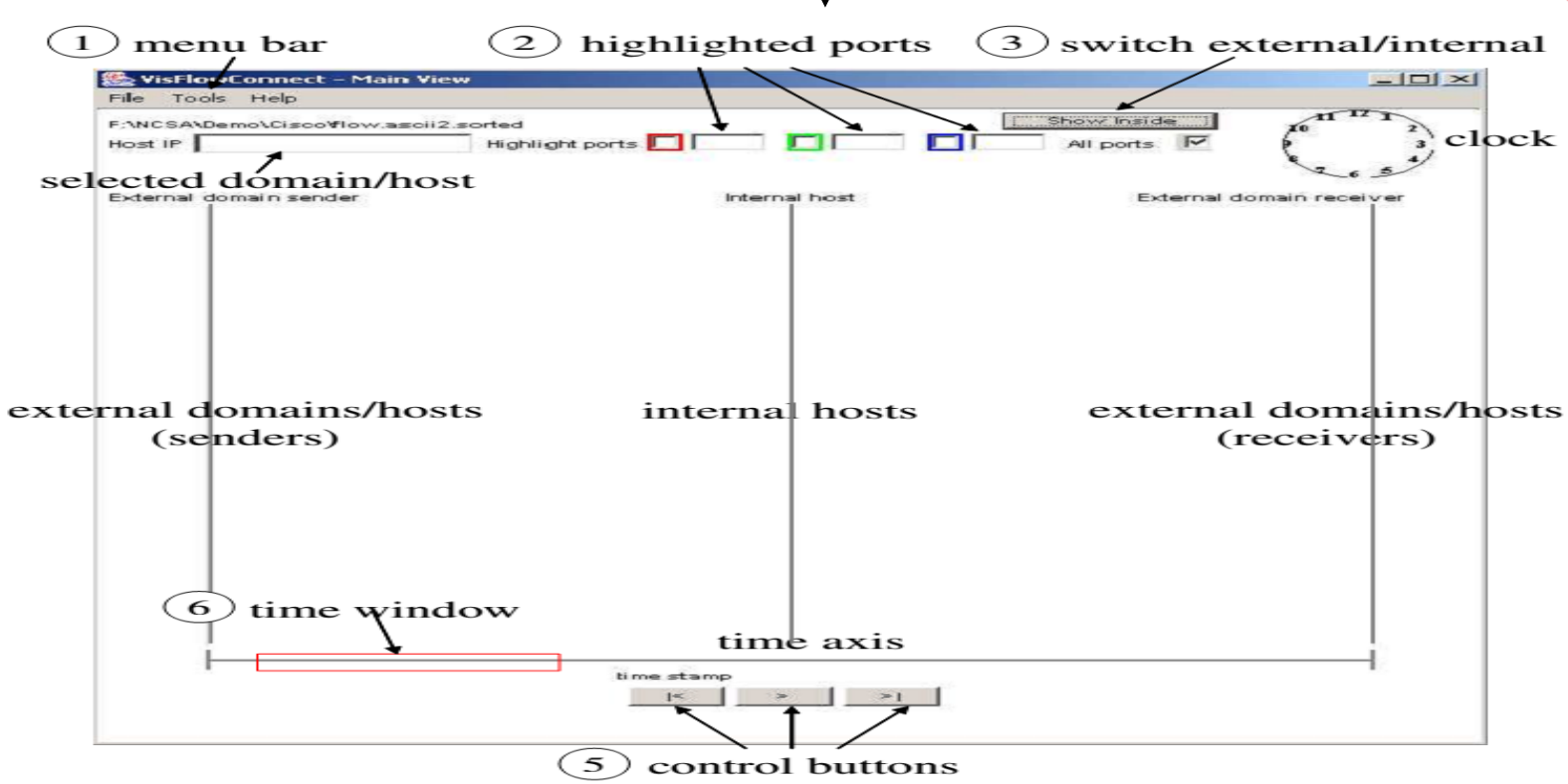


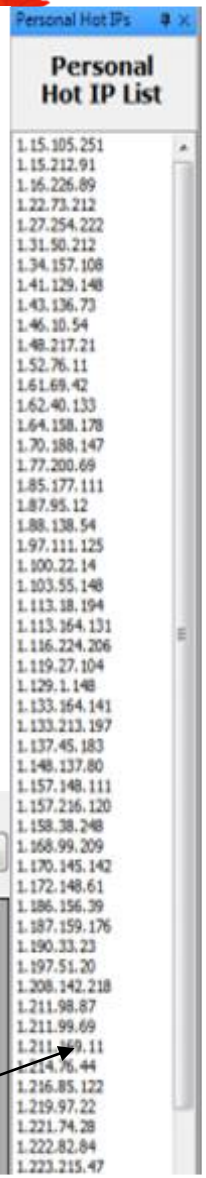


CyberSAVE - Research tool

Logs analysis

VisFlowConnect-IP - Research tool





Viewing details for: **Source IP.IP-Address = 145.126.46.39**

Show: Row ID / Cluster Count — Configure

	Bytes	Source IP.IP-Address	Source Port	Destination IP.IP-Address	Destination Port	Source Country.Lower	Start Time	Cluster Count
▶	58	145.126.46.39	59770	160.97.11.68	53	united states	5/2/2010 12:09:...	1
	62	145.126.46.39	10336	195.227.68.225	53	united states	5/2/2010 12:10:...	1
	62	145.126.46.39	44910	175.191.232.14	53	united states	5/2/2010 12:10:...	1
	124	145.126.46.39	32437	151.240.87.204	53	united states	5/2/2010 12:10:...	1
	138	145.126.46.39	18020	160.97.249.29	53	united states	5/2/2010 12:06:...	1

VIAssist - Commercial tool

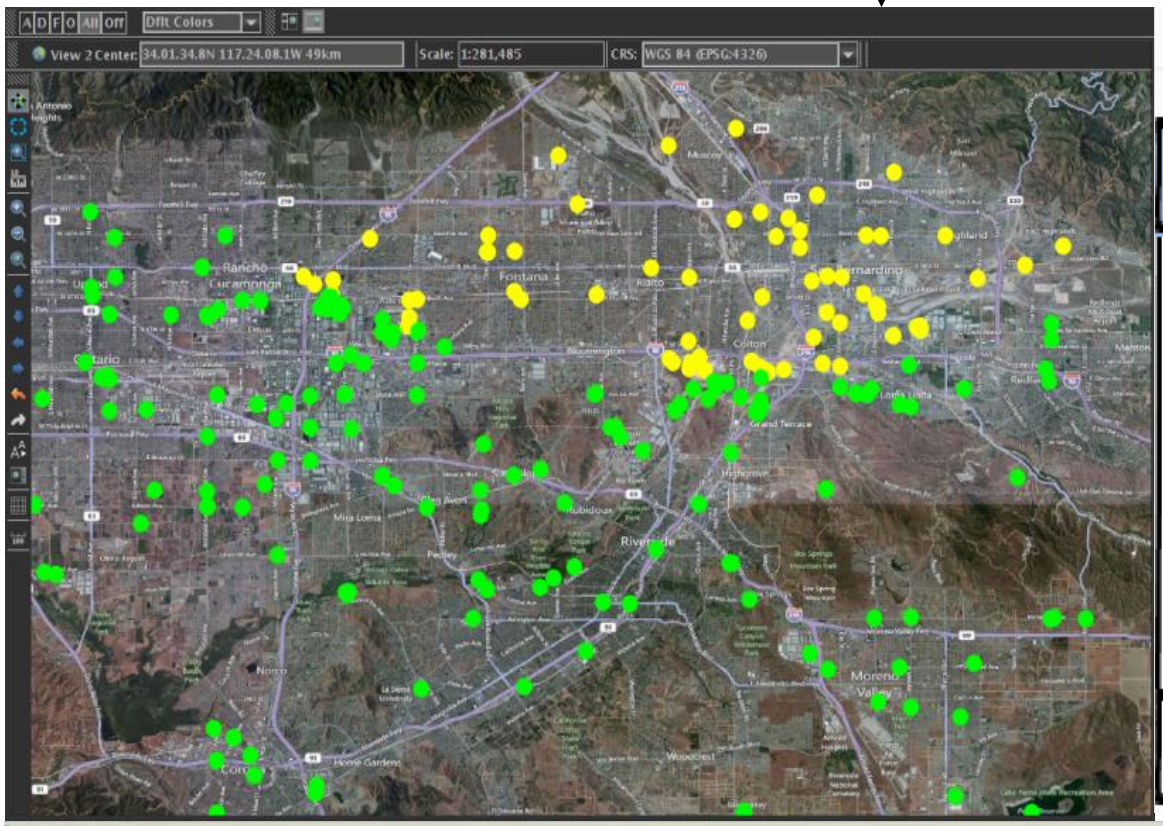
Proactive - Reactive model

This model consider how the tool responds to possible attacks, so we can think of a proactive model that is comprehensive of automatic solutions and of a reactive model that comprehend semi-automatic solutions (that require the action of a cyber operator)

Each of the two model is made mainly by three parts, one for the attacks, one for the situation and one for the (proposed or automatic) solutions

Proactive model

CyberSAVE - Research tool

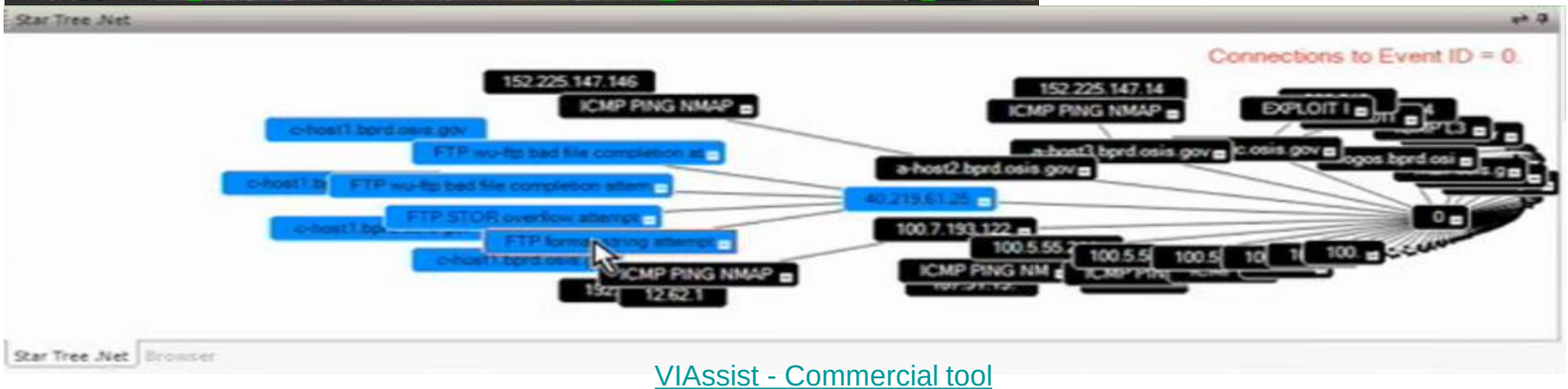


Automatic solutions

Successful operation in green

Unsuccessful operation in red

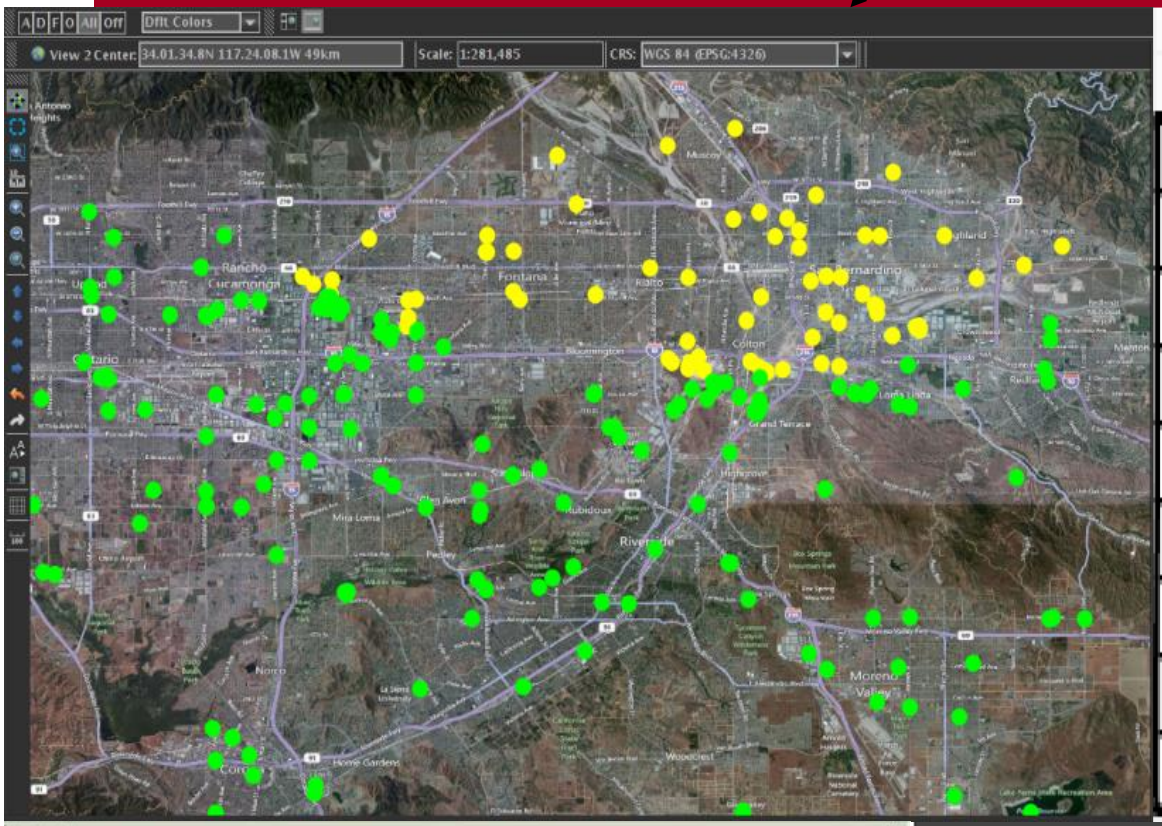
Why



VIAssist - Commercial tool

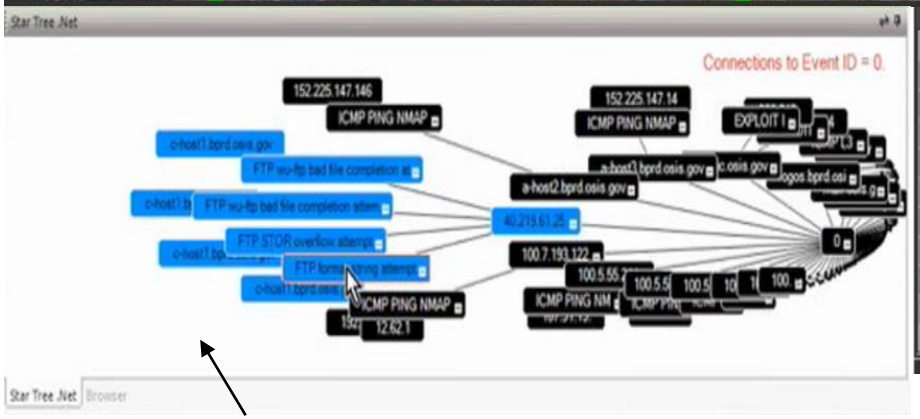
Reactive model

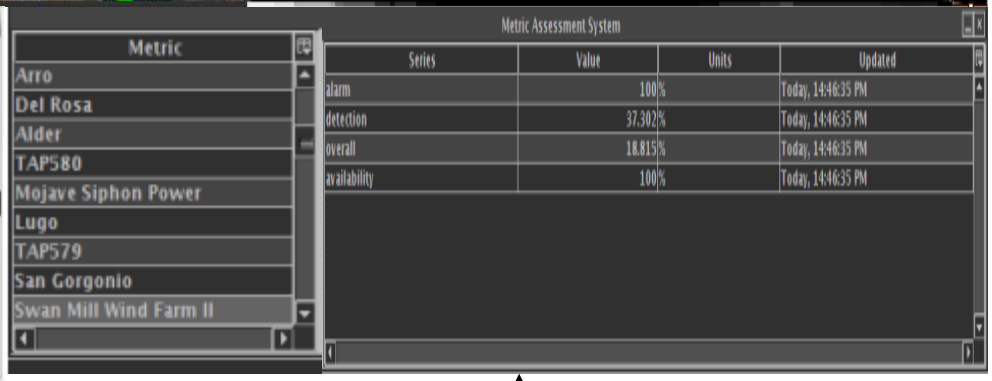
CyberSAVE - Research tool



Suggested solutions

Solution	Effects	Approval index
Sol-1	"Textual effects"	95%
...	...	...
...	...	...
...	...	...
...	...	...
...	...	...
...	...	...
Sol-n	"effects of Sol-n"	1%





VIAssist - Commercial tool

CyberSAVE - Research tool

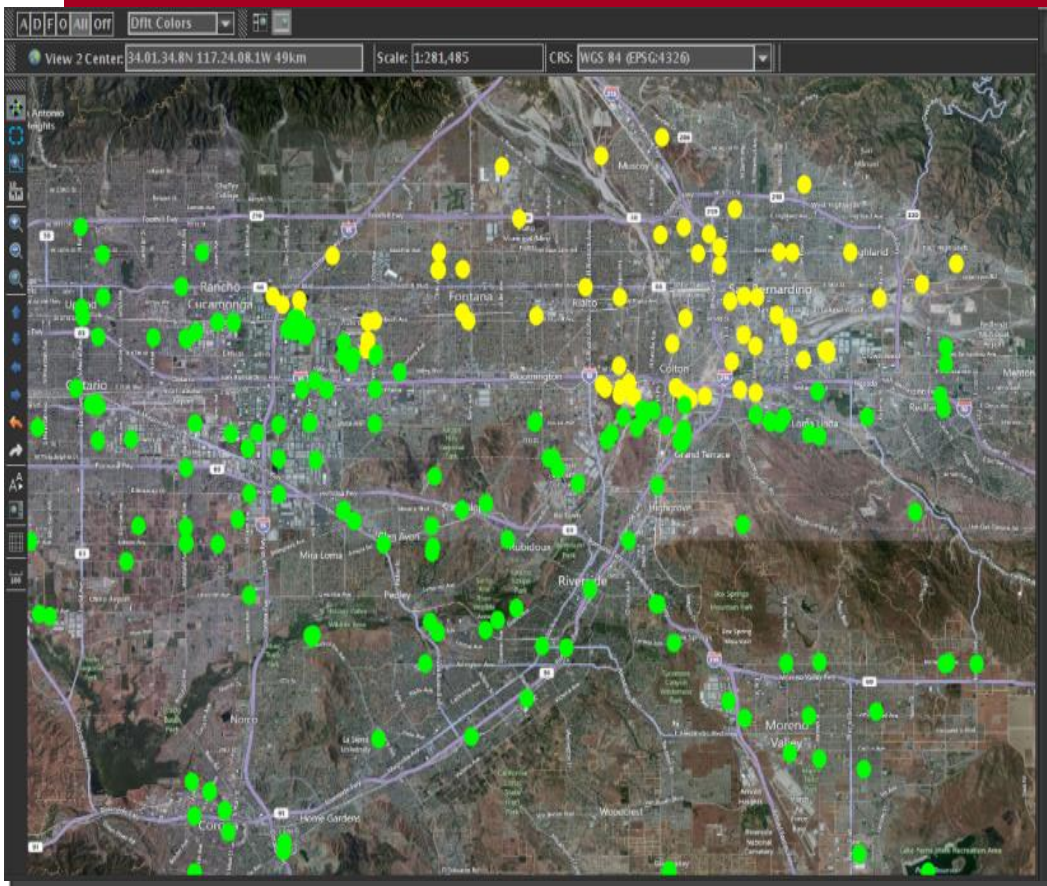
Mixed analysis model

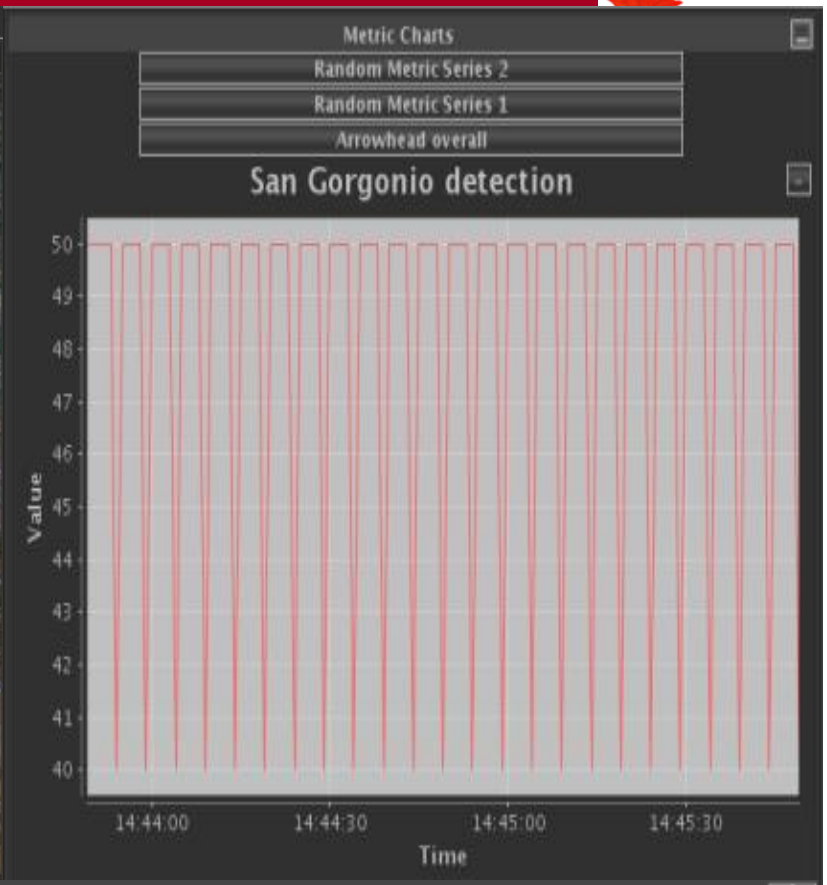
This is a model that divides the interface in the three main areas of interest :

- attack (model + effects)
- situation + risks
- solutions (automatic and semi-automatic)

Attack (model + effects)

CyberSAVE - Research tool





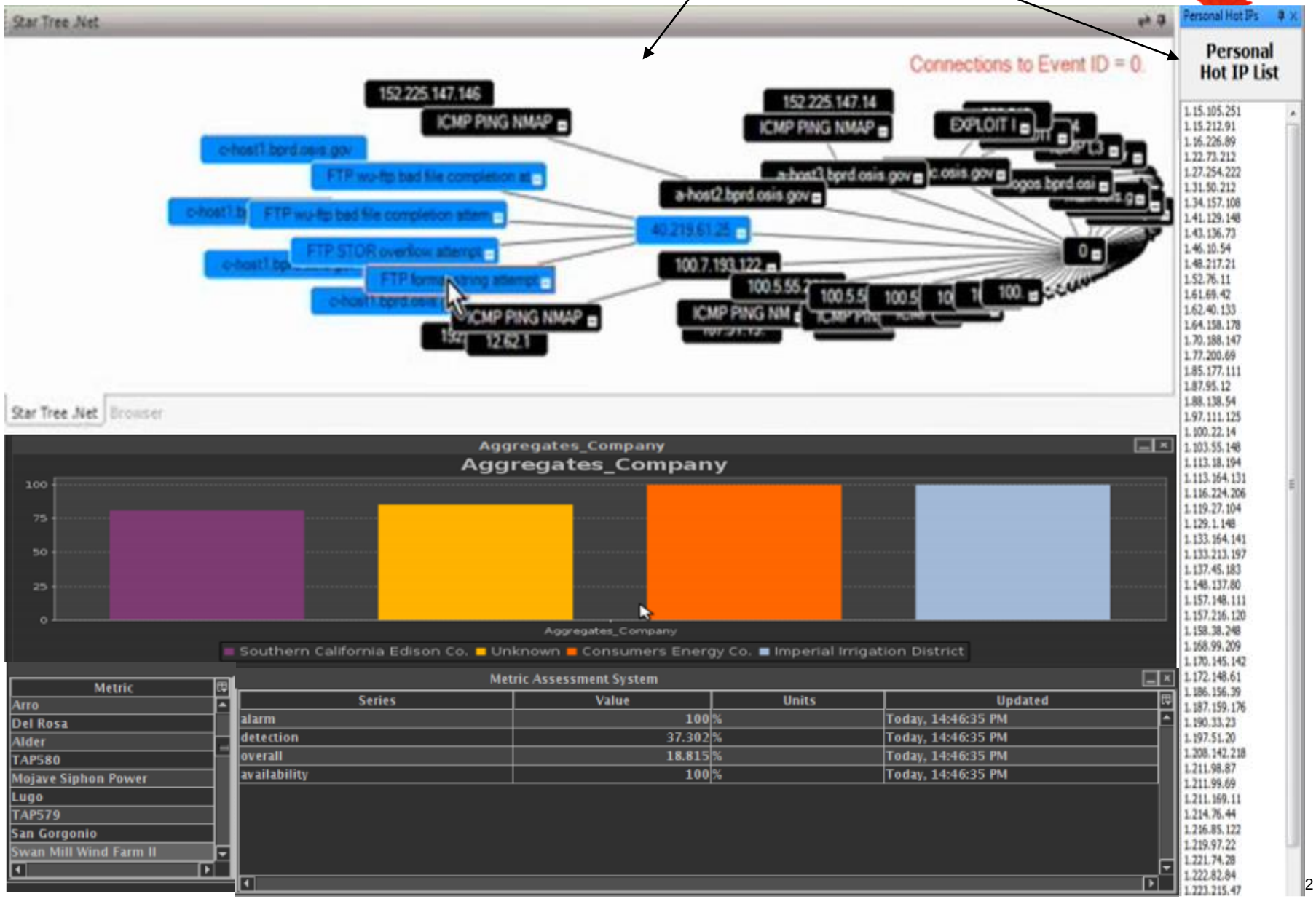
Metric Assessment System

Metric
Arro
Del Rosa
Alder
TAP580
Mojave Siphon Power
Lugo
TAP579
San Gorgonio
Swan Mill Wind Farm II

Series	Value	Units	Updated
alarm	100	%	Today, 14:46:35 PM
detection	37.302	%	Today, 14:46:35 PM
overall	18.815	%	Today, 14:46:35 PM
availability	100	%	Today, 14:46:35 PM

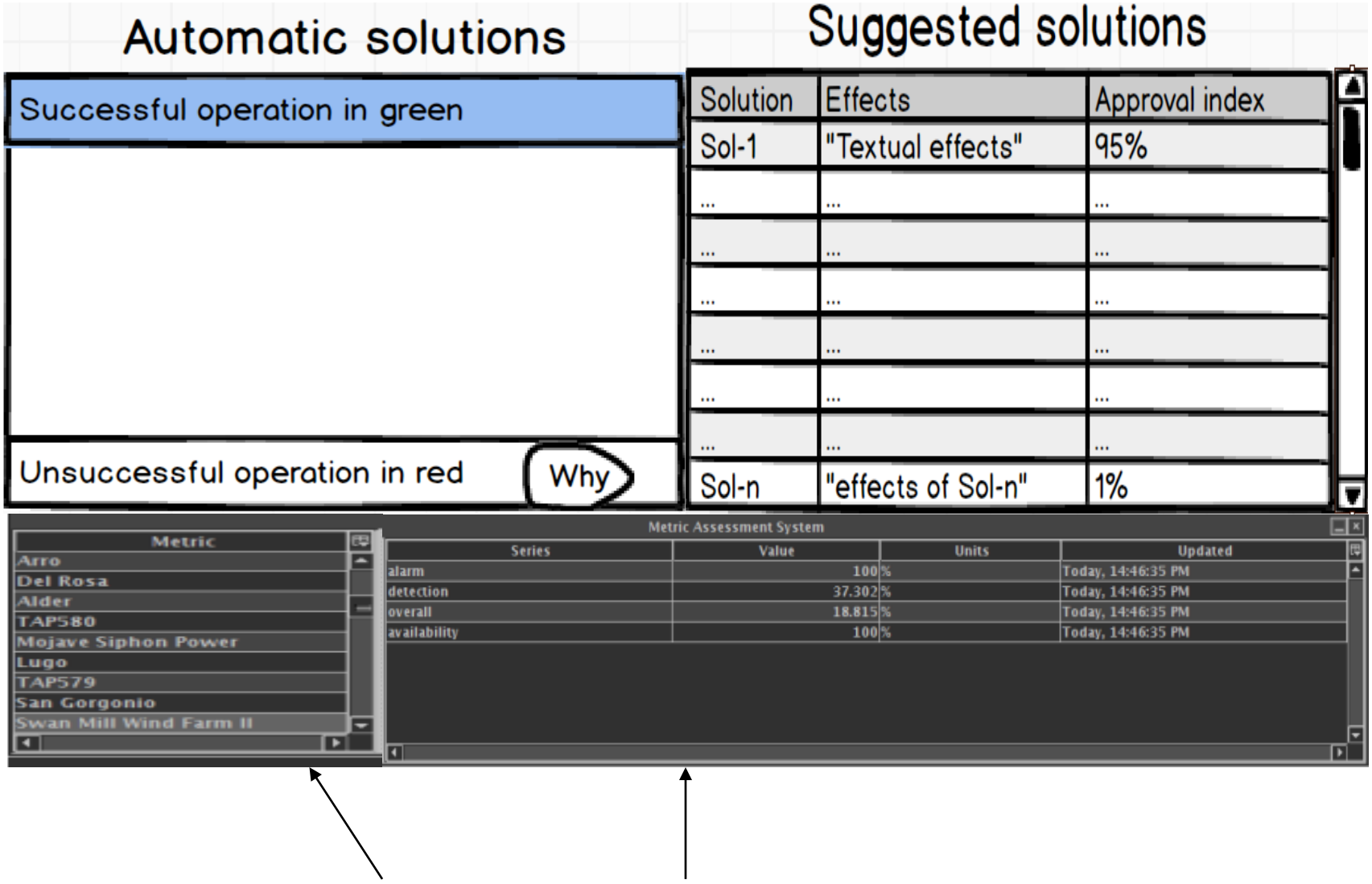
Situation + Risks

VIAssist - Commercial tool



CyberSAVE - Research tool

Solutions

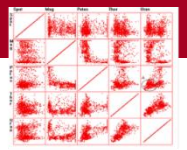
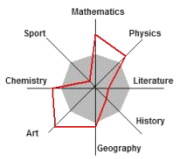


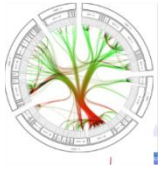
CyberSAVE - Research tool

Last but not least…

Basic theory

DATA → Internal **Representation**



Encoding of values
- Univariate data
- Bivariate data
- Trivariate data
- Multidimensional data

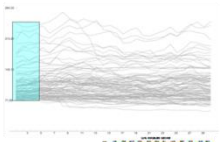
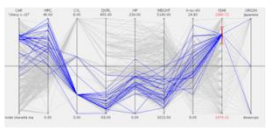
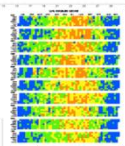
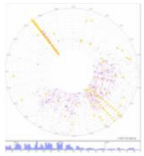
Encoding of relations

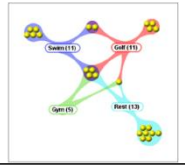
Temporal data

Map & Diagrams

Graphs/Trees

Data streams

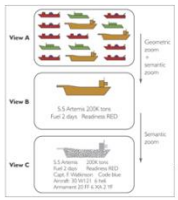
Internal **Representation**

Space limitations
- Scrolling
- Overview + details
- Distortion
- Suppression
- Zoom & pan
- Semantic zoom

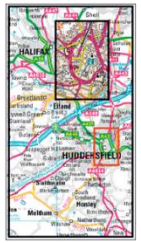
Time limitation

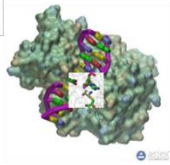
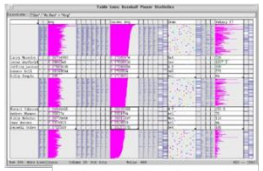
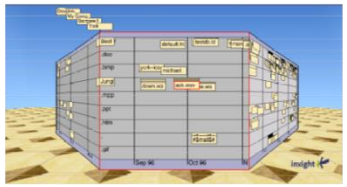
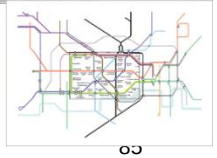
Perceptual issues

Cognitive issues

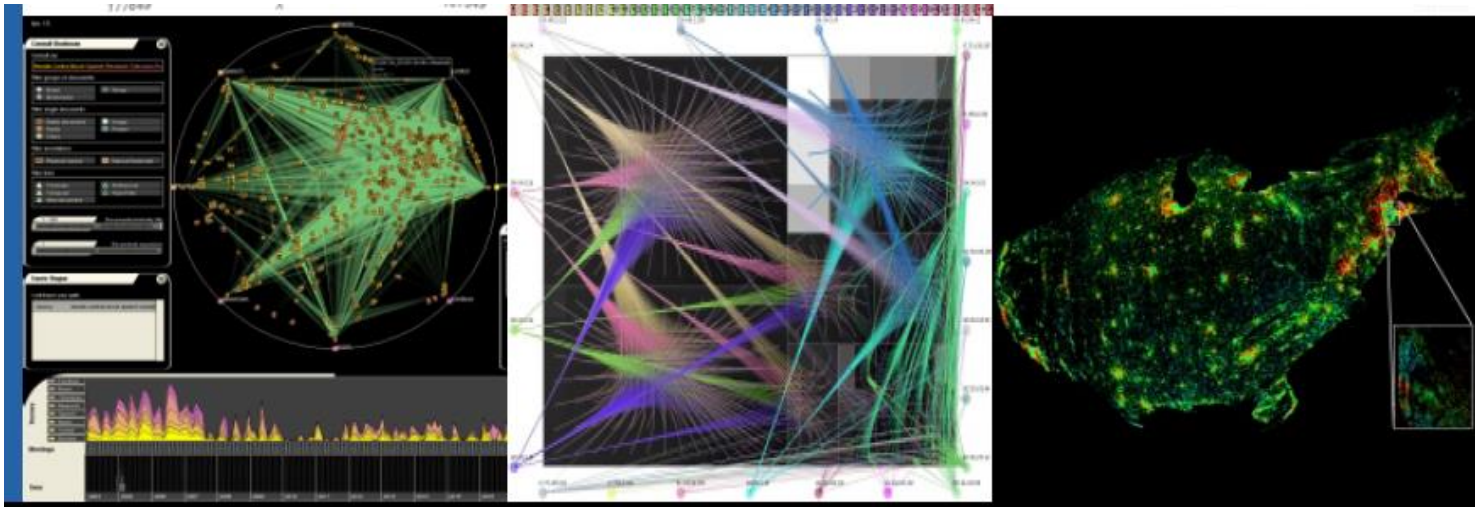


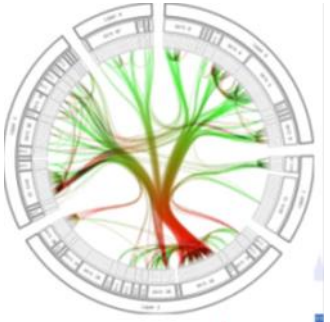
Presentation

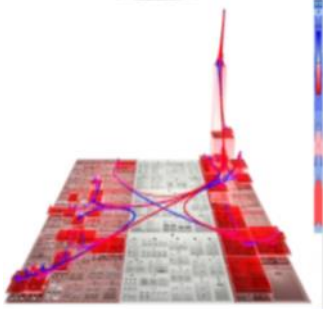


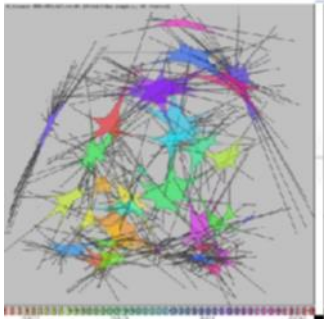





Well known solutions!









Density Estimation Over Data Stream*

Aoying Zhou
Dept. of Computer Science,
Fudan University
220 Handan Rd.
Shanghai, 200433, P.R. China
ayzhou@fudan.edu.cn

Zhiyuan Cai
Dept. of Computer Science,
Fudan University
220 Handan Rd.
Shanghai, 200433, P.R. China
zycai@fudan.edu.cn

Li Wei
Dept. of Computer Science,
Fudan University
220 Handan Rd.
Shanghai, 200433, P.R. China
lwei@fudan.edu.cn

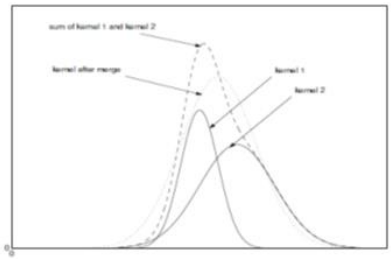


Figure 2: Kernel merging operation

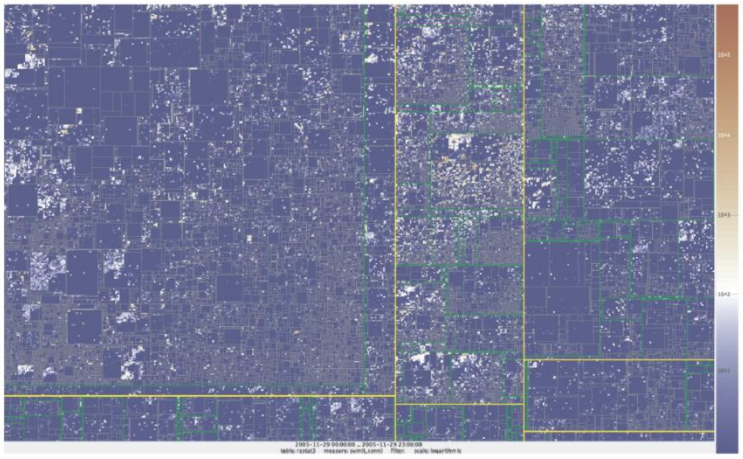
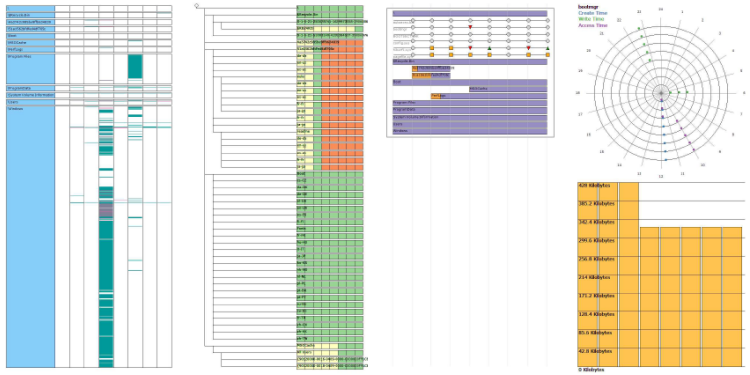


Fig. 5. Anonymized outgoing traffic connections from our university gateway on November 29th, 2005 showing all 197427 IP prefixes.

New research ideas

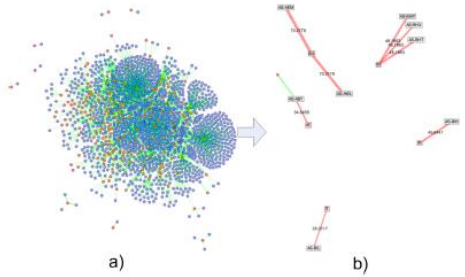
ICPS Published by ACM
ACM INTERNATIONAL CONFERENCE PROCEEDINGS SERIES

VizSec 2013



(a) Overview (b) Treeview (c) Directory Content (d) Metadata

Figure 1: The Change-Link 2.0 user interface is comprised of four linked views. The *Overview* window supports quick browsing by highlighting locations where data has changed within each time period. The *TreeView* window shows how the directory-tree structure has changed over time. The *Directory Content* window shows how all of the files and directories within a selected directory have changed over time. The *Metadata* window uses a polar plot and bar graph to reveal patterns of change for a selected file or directory.



a) b)

Figure 2: *Feature graph view* of the CGLZ feature, before (a) and after (b) the application of the threshold values. Red color represents the selected edges.

Proceedings of the Tenth Workshop on
Visualization for Cyber Security

Atlanta, Georgia, USA
October 14, 2013

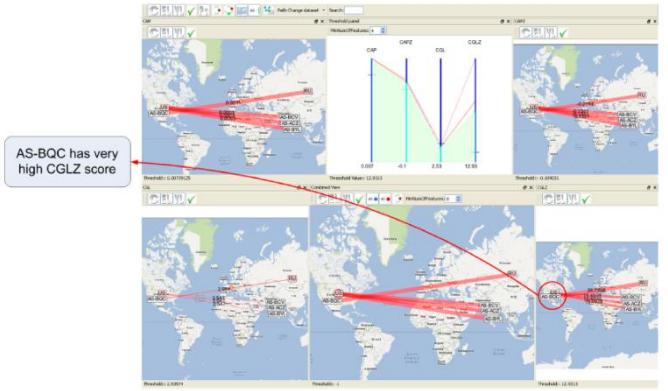


Figure 5: BGPfuse visualization of the successful BGP path change events (W_{pc}) that occurred on 24-Aug-2011, after the application of filtering. The set of selected thresholds is $T = \{(t_{CAP}, t_{CAPZ}, t_{CGL}, t_{CGLZ}) = (0.007, -0.109, 2.53, 12.93)\}$

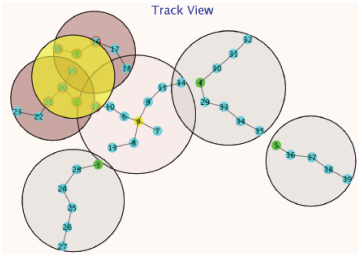


Figure 7: An example of jamming attack on nodes 1,2, 12, 15, 16, 19, 20, and 21.

Thanks for your attention!

Questions?