Visual Analysis of Corporate Network Intelligence: Abstracting and Reasoning on Yesterdays for Acting Today

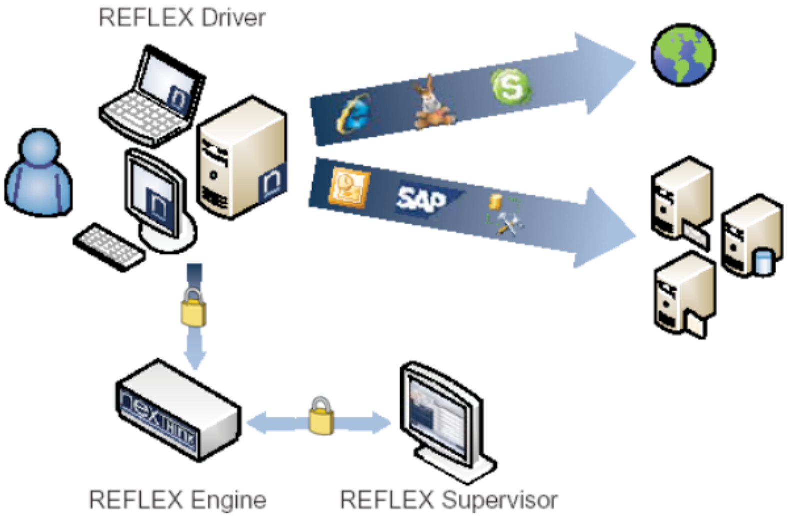
Denis Lalanne, Enrico Bertini
University of Fribourg
Fribourg, Switzerland

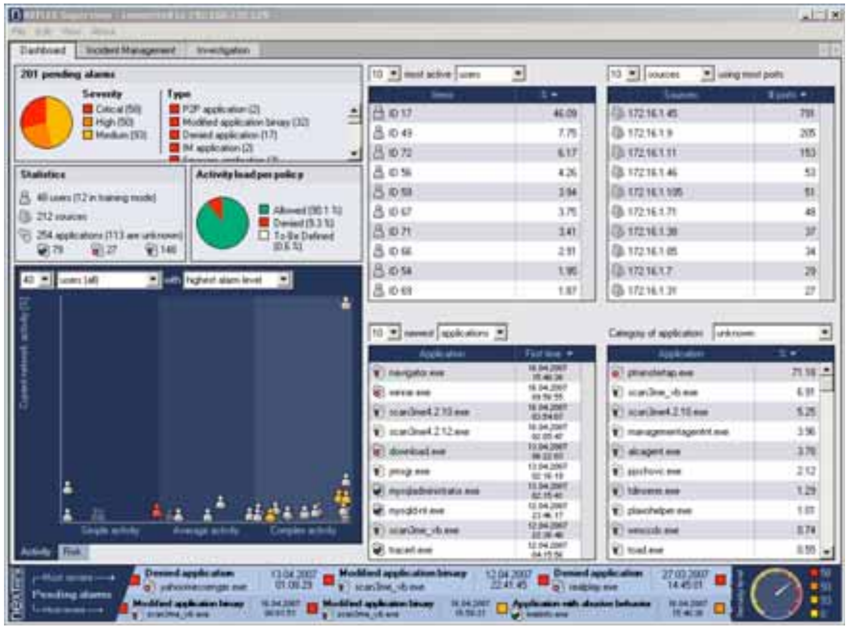
Patrick Hertzog, Pedro Bados
NEXThink S.A.
Lausanne, Switzerland

October 29, 2007

VizSec 2007 - Sacramento, CA USA

Starting point: NEXThink Supervisor





201 pending alarms

Severity
- 🟥 Critical (58)
- 🟧 High (50)
- 🟨 Medium (93)

Type
- 🟥 P2P application (2)
- 🟥 Modified application binary (32)
- 🟥 Denied application (17)
- 🟥 IM application (2)

Statistics
- 48 users (12 in training mode)
- 212 sources
- 254 applications (113 are unknown)
- 79 27 148

Activity load per policy
- 🟩 Allowed (90.1 %)
- 🟥 Denied (9.3 %)
- □ To-Be Defined (0.6 %)

40 users (all) with highest alarm level

10 most active users

Users	Σ
ID 17	46.09
ID 49	7.75
ID 72	6.17
ID 56	4.26
ID 59	3.94
ID 67	3.75
ID 71	3.41
ID 66	2.91
ID 54	1.95
ID 69	1.87

10 sources using most ports

Sources	# ports
172.16.1.45	791
172.16.1.9	205
172.16.1.11	153
172.16.1.46	53
172.16.1.105	51
172.16.1.71	48
172.16.1.38	37
172.16.1.85	34
172.16.1.7	29
172.16.1.31	27

10 newest applications

Application	First time
navigator.exe	16.04.2007 15:46:36
wevue.exe	16.04.2007 09:59:55
scan3net4.2.10.exe	16.04.2007 03:54:07
scan3net4.2.12.exe	16.04.2007 02:05:47
download.exe	13.04.2007 09:22:03
pmogr.exe	13.04.2007 02:16:13
mysqladministrator.exe	13.04.2007 02:15:40
mysqld-nt.exe	12.04.2007 23:46:17
scan3ne_vb.exe	12.04.2007 22:38:46
tracert.exe	12.04.2007 04:15:56

Category of application unknown

Application	Σ
pinandsetup.exe	71.58
scan3ne_vb.exe	6.91
scan3net4.2.10.exe	5.25
managementagentnt.exe	3.56
alcagent.exe	3.76
ppchovc.exe	2.12
tdtnsrmr.exe	1.29
plaxohelper.exe	1.07
wmccds.exe	0.74
load.exe	0.55

Pending alarms

Alarm	Application	Time
Denied application	yahoomessenger.exe	13.04.2007 01:06:29
Modified application binary	scan3ne_vb.exe	12.04.2007 22:41:45
Denied application	realplay.exe	27.03.2007 14:45:01
Modified application binary	scan3ne_vb.exe	16.04.2007 [illegible]
Modified application binary	scan3ne_vb.exe	16.04.2007 [illegible]
Application with abusive behaviour	[illegible].exe	16.04.2007 15:46:36

Hertzog, P. “*Visualizations to improve reactivity towards security incidents inside corporate networks*”.
In Proceedings of VizSEC '06.

Examples of raised questions we wanted to address

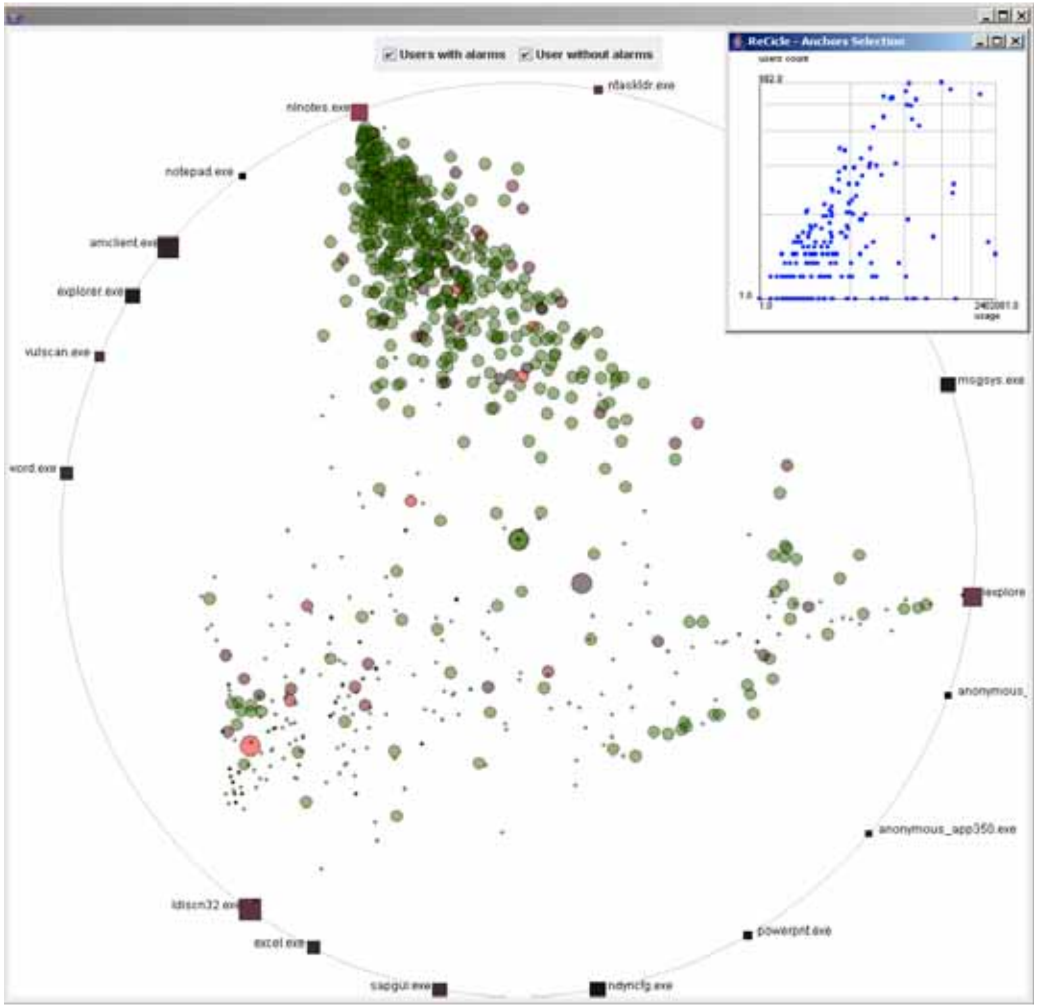
- *How do alarms distribute and evolve over time*?
  - More/less, peaks, patterns, …

- *How do alarms distribute over network resources*?
  - Which users do generate certain alarms? With what applications?

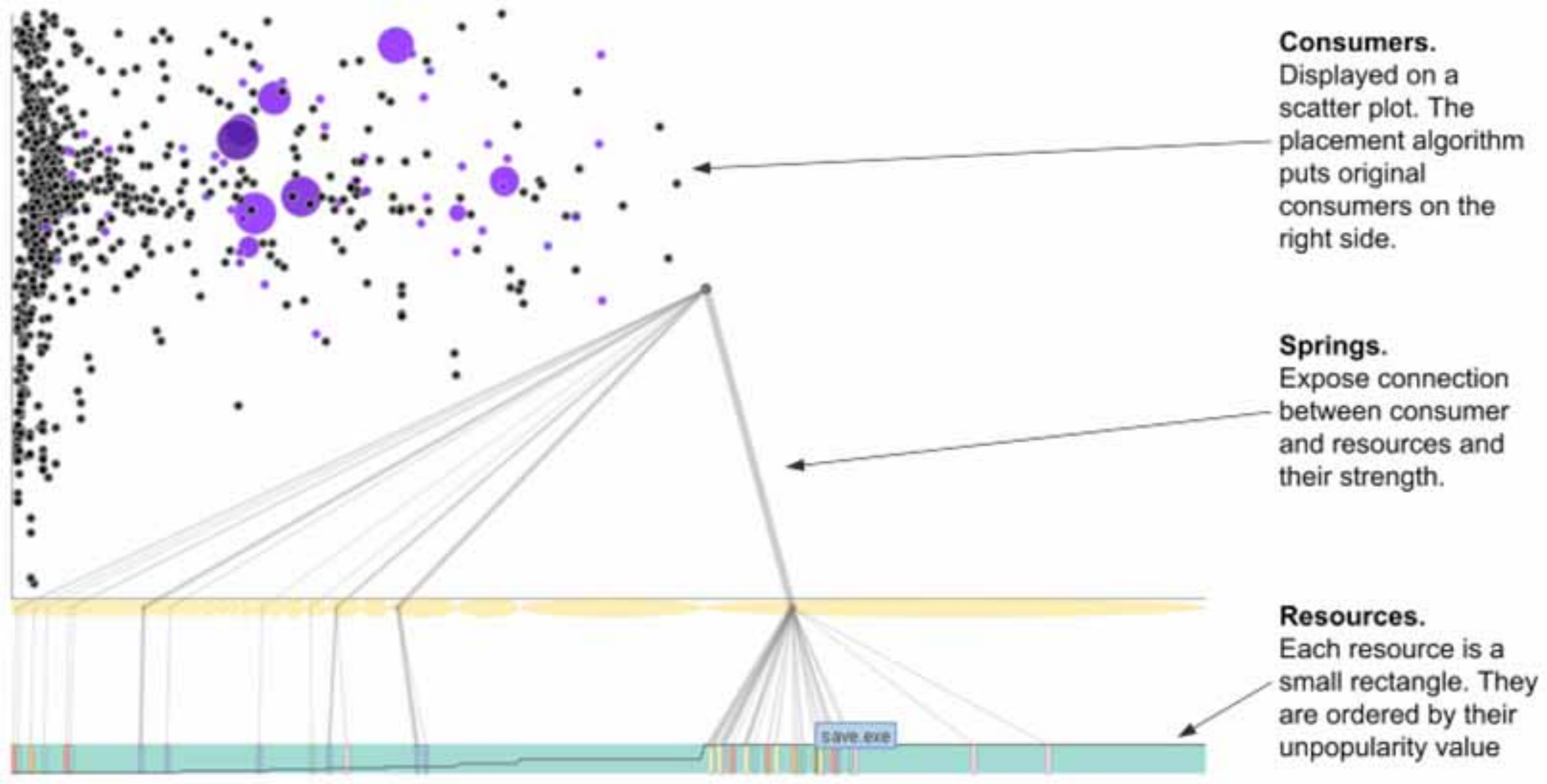
- *How can we segment the population in groups*?
  - in terms of the applications they use

- *How can we spot "original" behavior*?
  - What's original?

RadViz (aka Star Coordinates)



Originality View

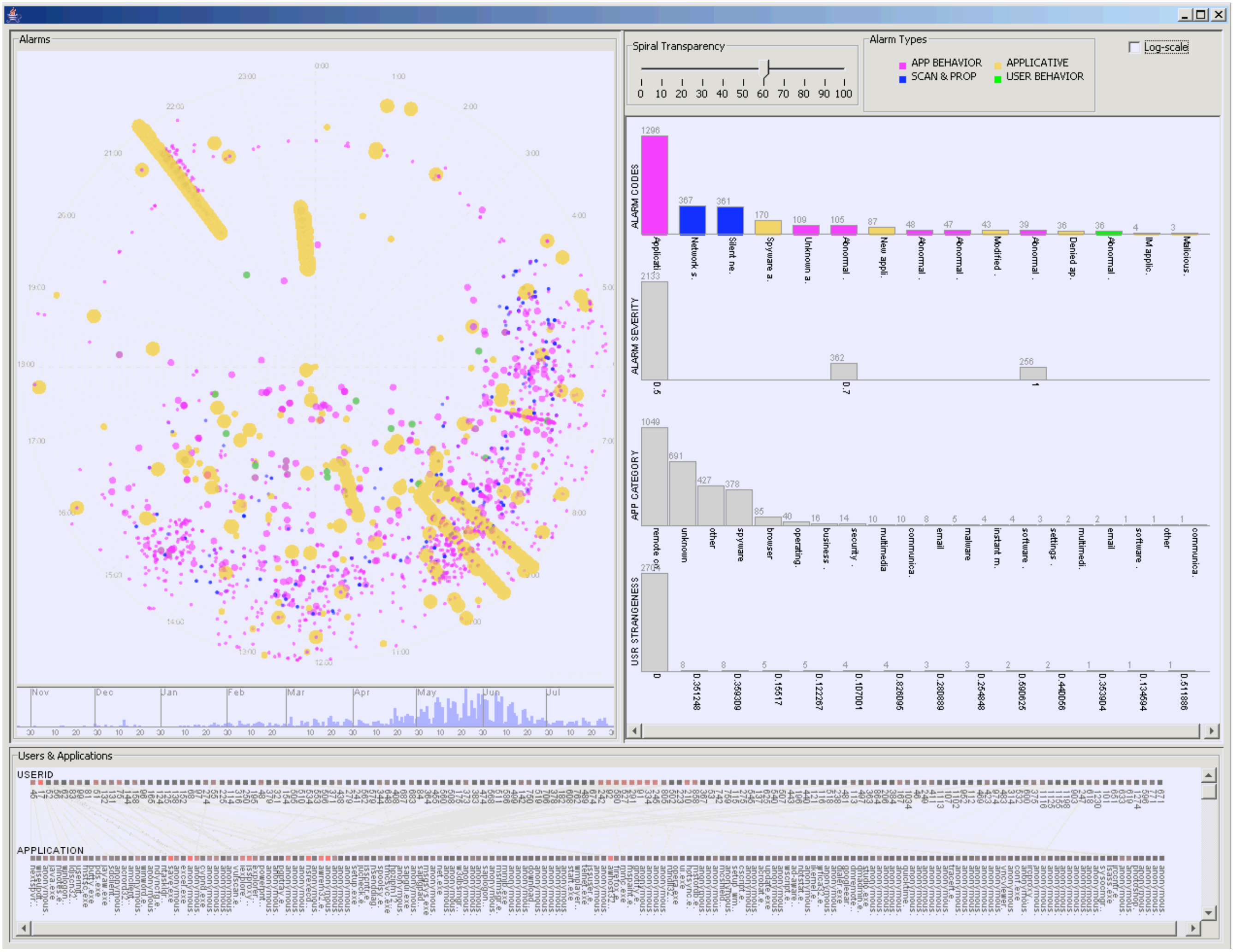


Consumers.
Displayed on a scatter plot. The placement algorithm puts original consumers on the right side.

Springs.
Expose connection between consumer and resources and their strength.

Resources.
Each resource is a small rectangle. They are ordered by their unpopularity value

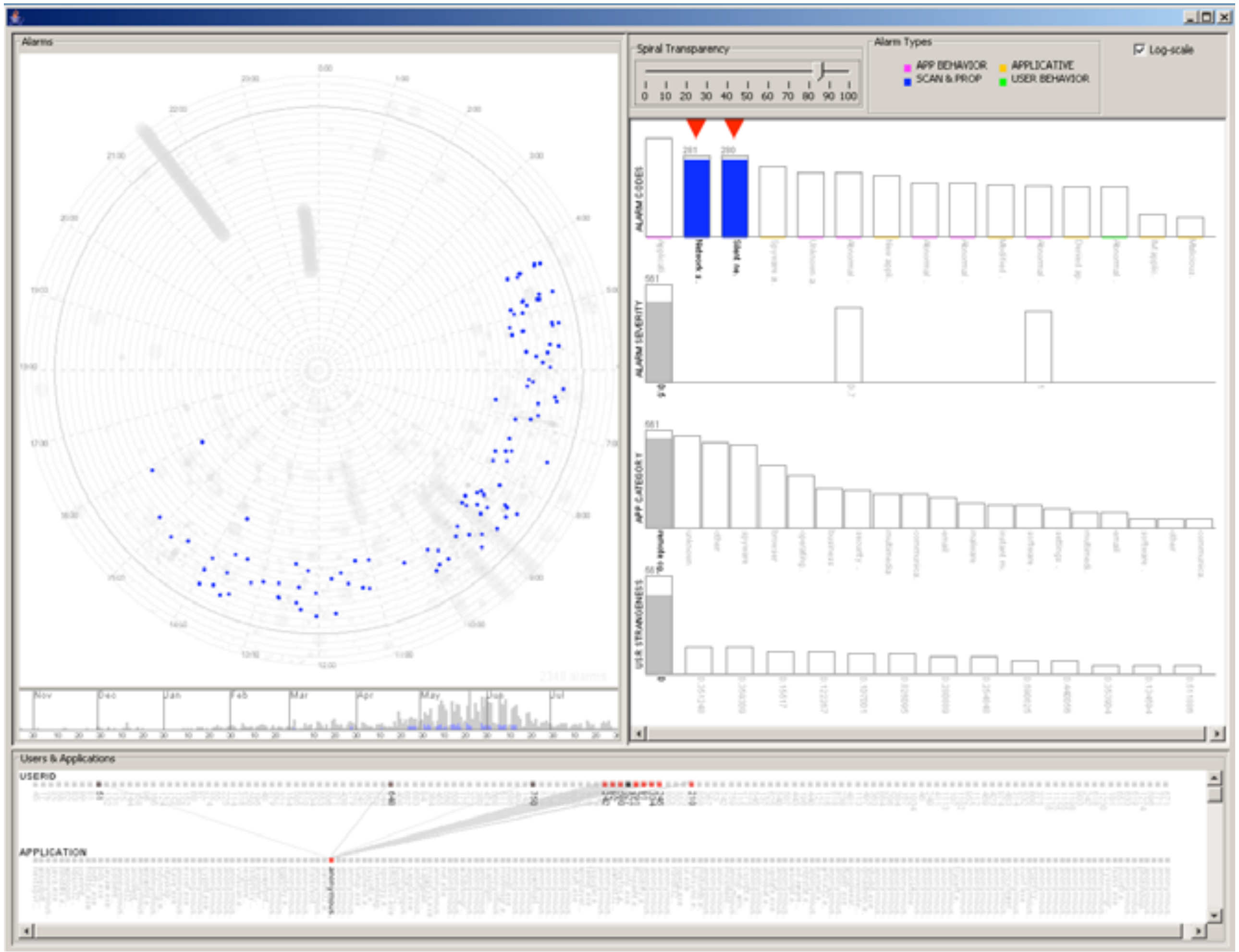
SpiralView


Alarms
0:00
1:00
2:00
3:00
4:00
5:00
7:00
8:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Spiral Transparency
0 10 20 30 40 50 60 70 80 90 100
Alarm Types
APP BEHAVIOR
APPLICATIVE
SCAN & PROP
USER BEHAVIOR
Log-scale
ALARM CODES
1296 Applicati
367 Network s.
361 Silent ne.
170 Spyware a.
109 Unknown a.
105 Abnormal .
87 New appli.
48 Abnormal .
47 Abnormal .
43 Modified .
39 Abnormal .
36 Denied ap.
36 Abnormal .
4 IM applic.
3 Malicious.
ALARM SEVERITY
2133 0.5
362 0.7
256 1
APP CATEGORY
1049 remote co
691 unknown
427 other
378 spyware
85 browser
40 operating.
16 business .
14 security .
10 multimedia
10 communica.
8 email
5 malware
4 instant m.
4 software .
3 settings .
2 multimedi.
2 email
1 software .
1 other
1 communica.
USR STRANGENESS
2704 0
8 0.351248
8 0.359309
5 0.15517
5 0.122267
4 0.107001
4 0.826095
3 0.280889
3 0.254848
2 0.590625
2 0.440056
1 0.353904
1 0.134694
1 0.511886
Users & Applications
USERID
APPLICATION

Analysis patterns

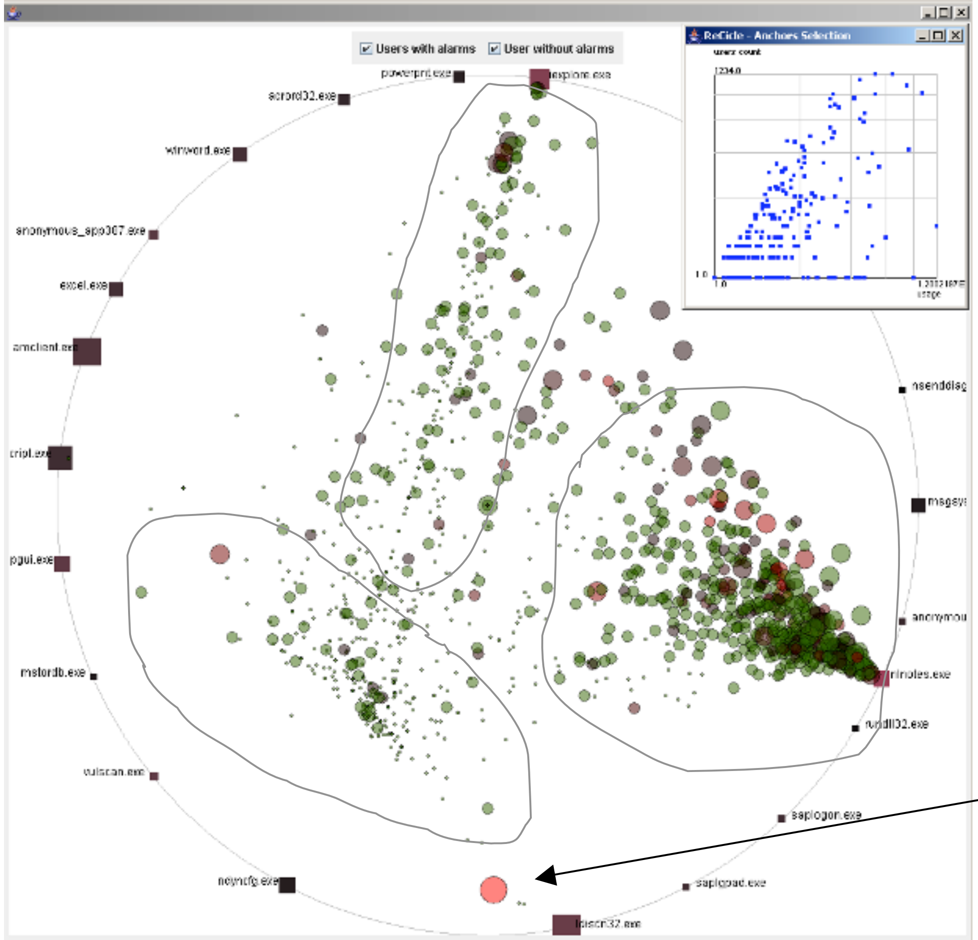
- Segmentation
  - Who does what
- Correlation, clustering, outliers
  - Building profiles
- Alerts as an entry point to the whole population
  - Normal vs. abnormal behavior
- Tracking and evolution

Segmentation



☑ Log-scale

Correlation, clustering, outliers

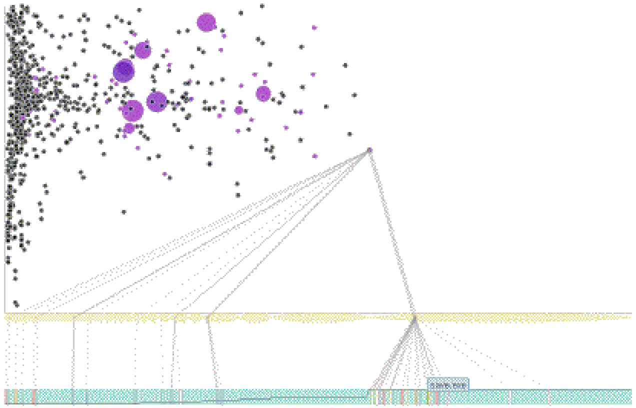


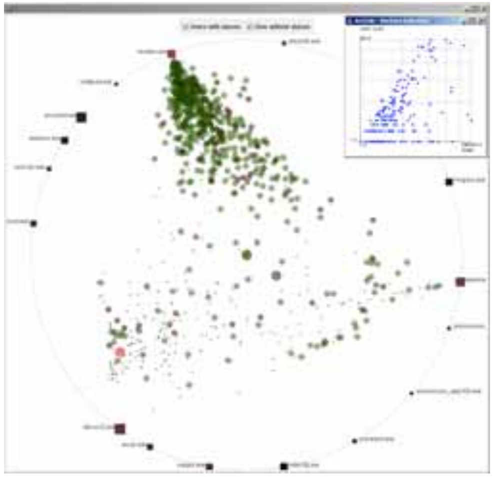
☑ Users with alarms ☑ User without alarms

Clusters

Outlier

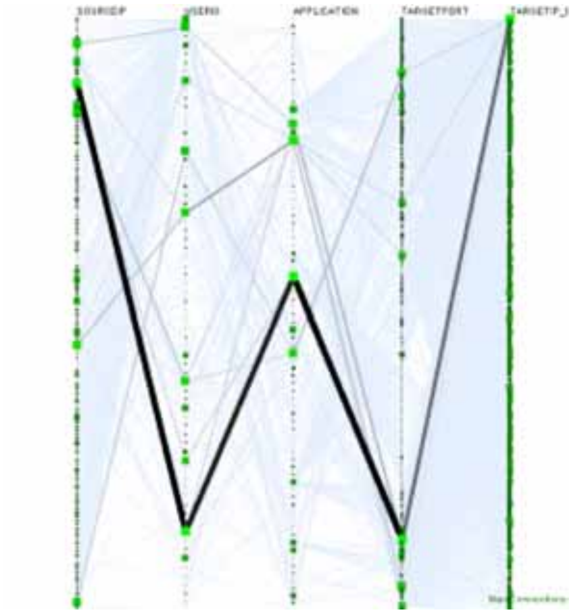
Alerts as an entry point



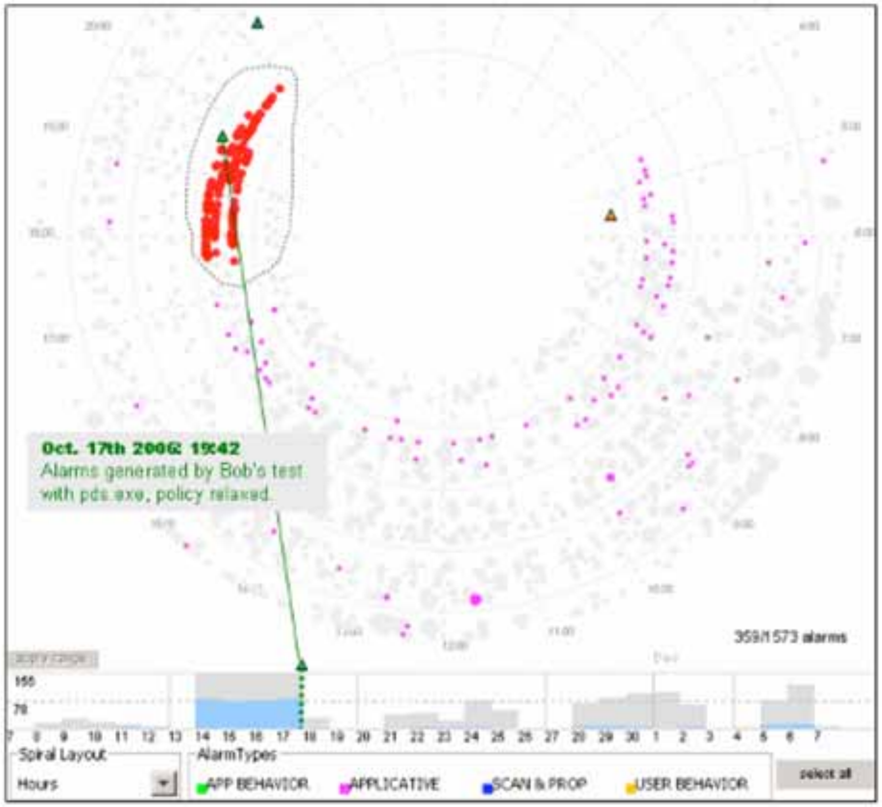


with vs. without alarms

Signatures



Tracking and evolution



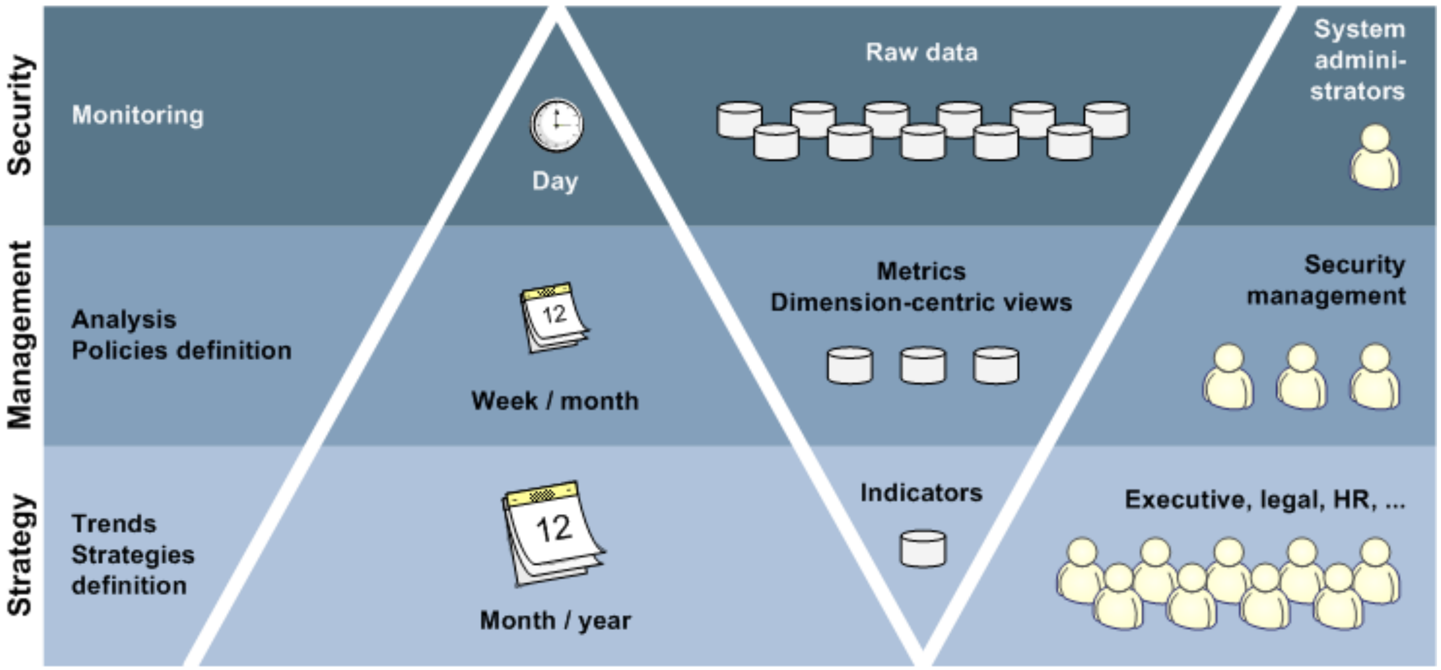
Oct. 17th 2006: 15:42
Alarms generated by Bob's test with pds.exe, policy relaxed.

359/1573 alarms

Spiral Layout: Hours

A wider perspective

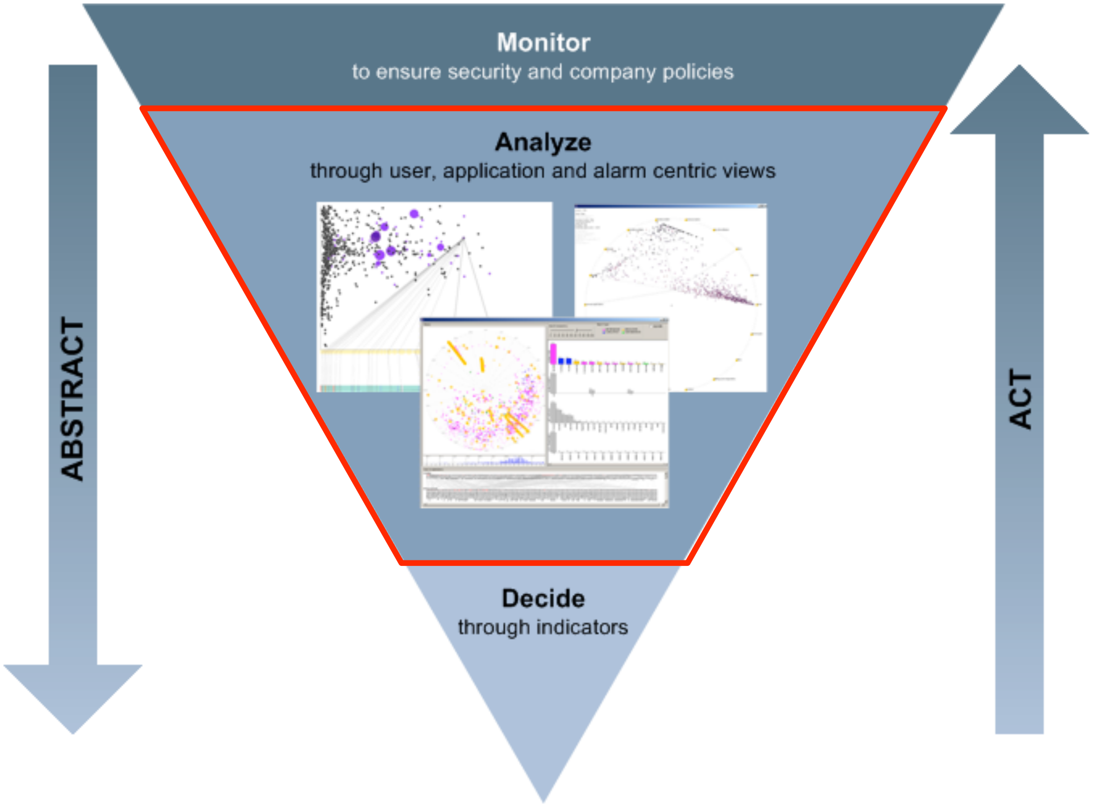
tasks, time scales, data abstraction, user types



	TASK	TIME SCALE	DATA ABSTRACTION	USER TYPE
Security	Monitoring	Day	Raw data	System administrators
Management	Analysis Policies definition	Week / month	Metrics Dimension-centric views	Security management
Strategy	Trends Strategies definition	Month / year	Indicators	Executive, legal, HR, ...

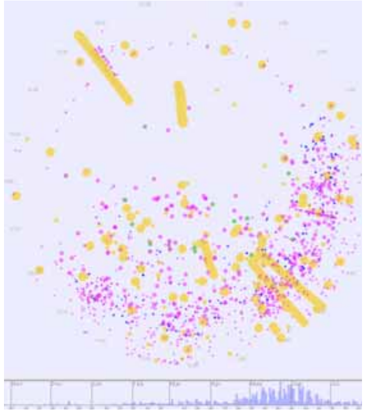
The need to support visual analysis

- Explorative
  - Not completely formulated goals
  - From the middle layer to the top/bottom layers
- Explicative
  - Request to explain investigate events/trends

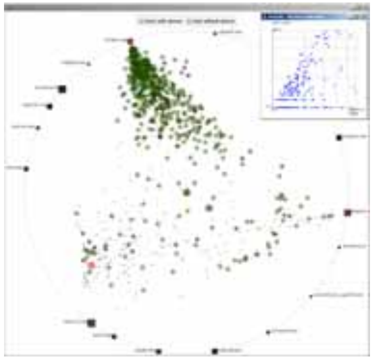

Monitor
to ensure security and company policies
Analyze
through user, application and alarm centric views
Decide
through indicators
ABSTRACT
ACT

Analysis and time

- Time explicit visualizations
  - Trending, time patterns, comparisons
  - Types:
    - Events (points and intervals)
    - Aggregated measures (count, sum, avg, etc.)
    - Composite metrics (e.g., risk)



- Time implicit visualizations
  - Relationships between entities (e.g., users and target IPs)
  - A time range must be selected
    - Tightly connected to performance
    - Too large ranges might be meaningless
  - How to represent evolution in time then?



Open issues

- Data explosion
  - Data reduction
  - Data/Visual aggregation
  - Interactivity
- Many small vs. one integrated tool
  - Plug-ins
  - Personalization
- Communication and data sharing between layers

Why so few attempts to address this wider perspective in VizSec?

Questions (... and Answers)?