Putting Security in Context

Visual Correlation of Network Activity with Real-World Information

Bill Pike, Chad Scherrer, & Sean Zabriskie
Pacific Northwest National Laboratory

bill.pike@pnl.gov

Battelle

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

What is the goal of analysis?

Use…

To find…

What is the goal of analysis?

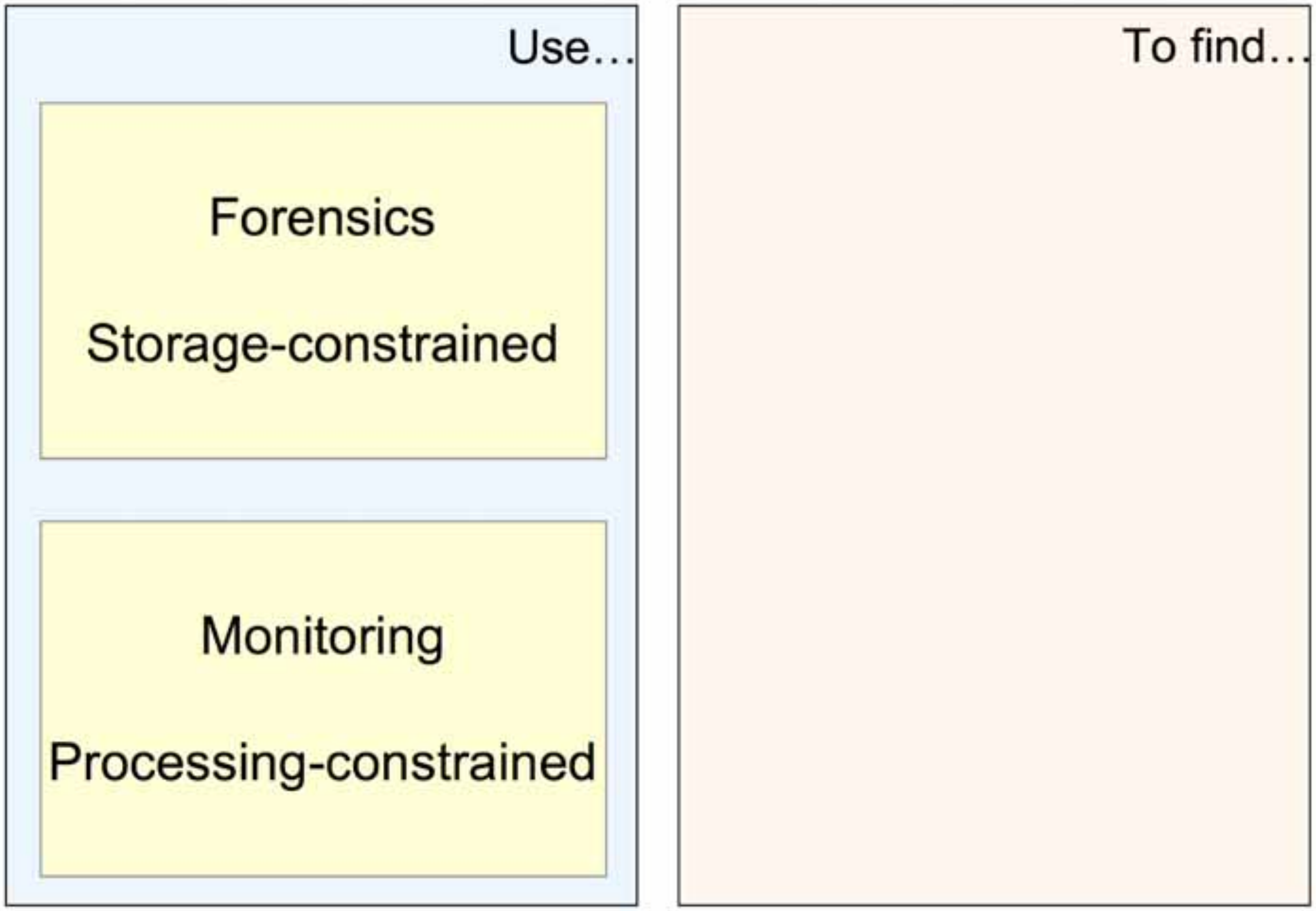
Use…

Forensics

Storage-constrained

To find…

What is the goal of analysis?



Use…

Forensics

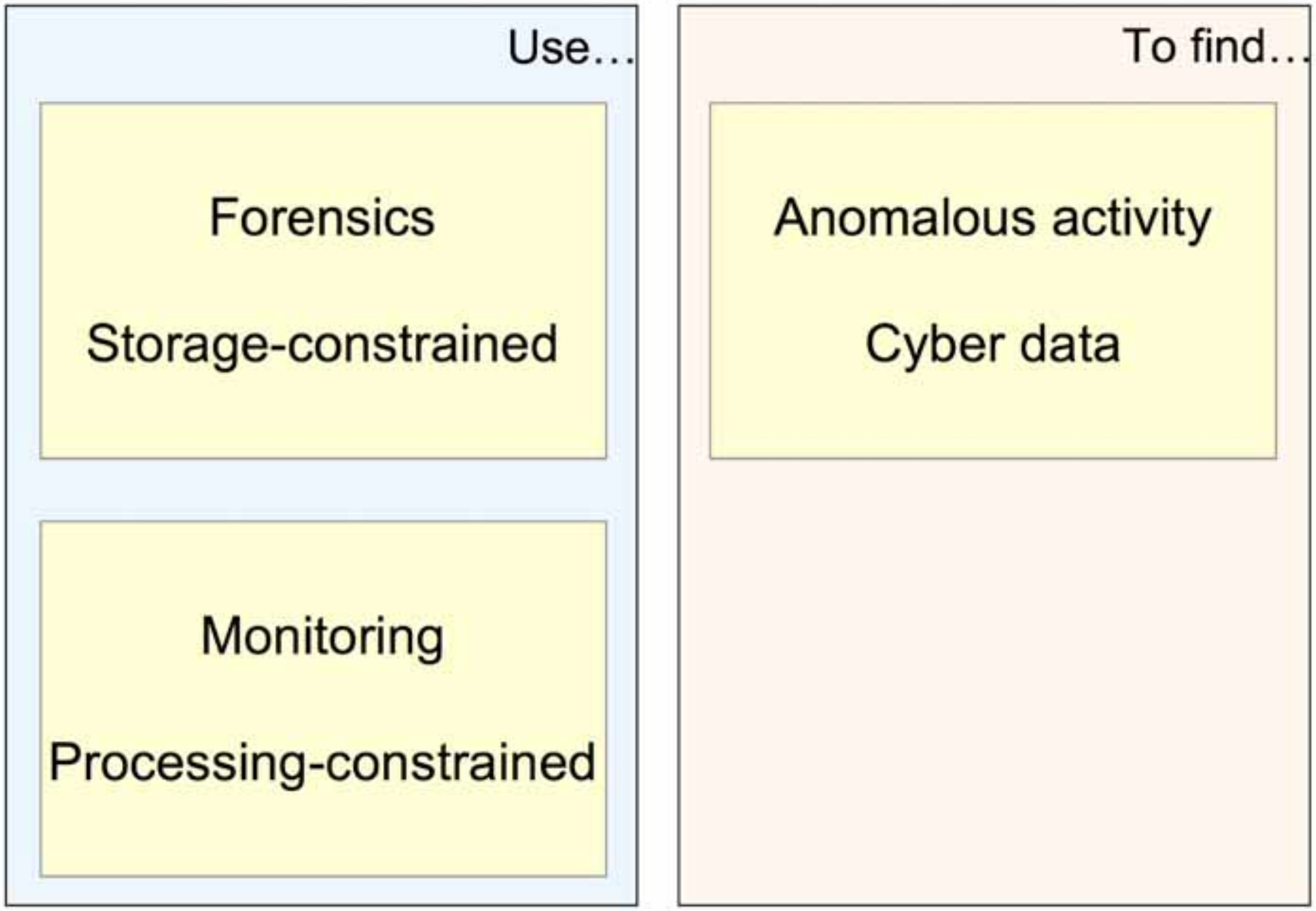
Storage-constrained

Monitoring

Processing-constrained

To find…

What is the goal of analysis?



Use…

Forensics

Storage-constrained

Monitoring

Processing-constrained

To find…

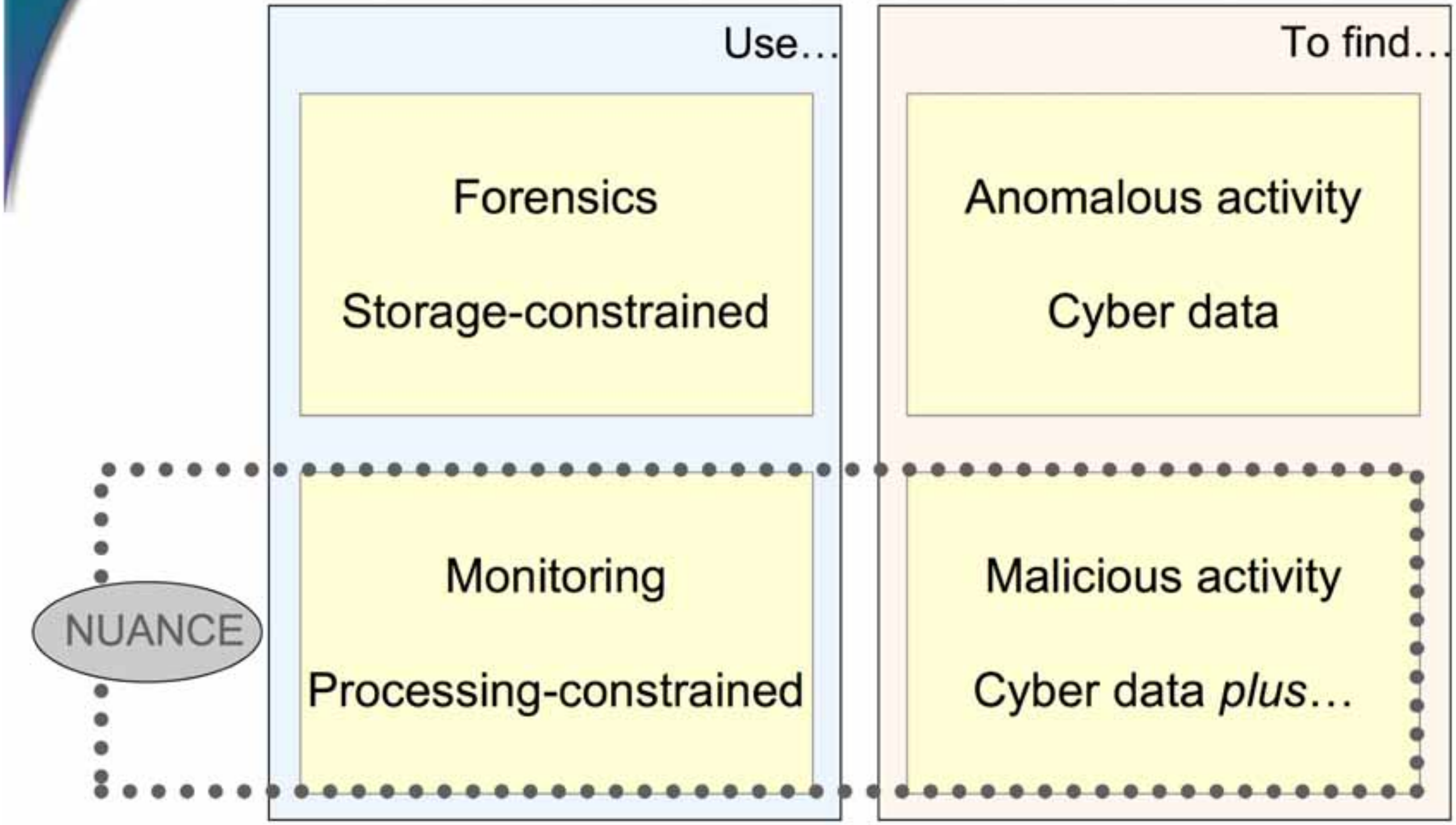
Anomalous activity

Cyber data

What is the goal of analysis?

Use…	To find…
Forensics Storage-constrained	Anomalous activity Cyber data
Monitoring Processing-constrained	Malicious activity Cyber data *plus*…

What is the goal of analysis?



Use…

Forensics

Storage-constrained

Monitoring

Processing-constrained

To find…

Anomalous activity

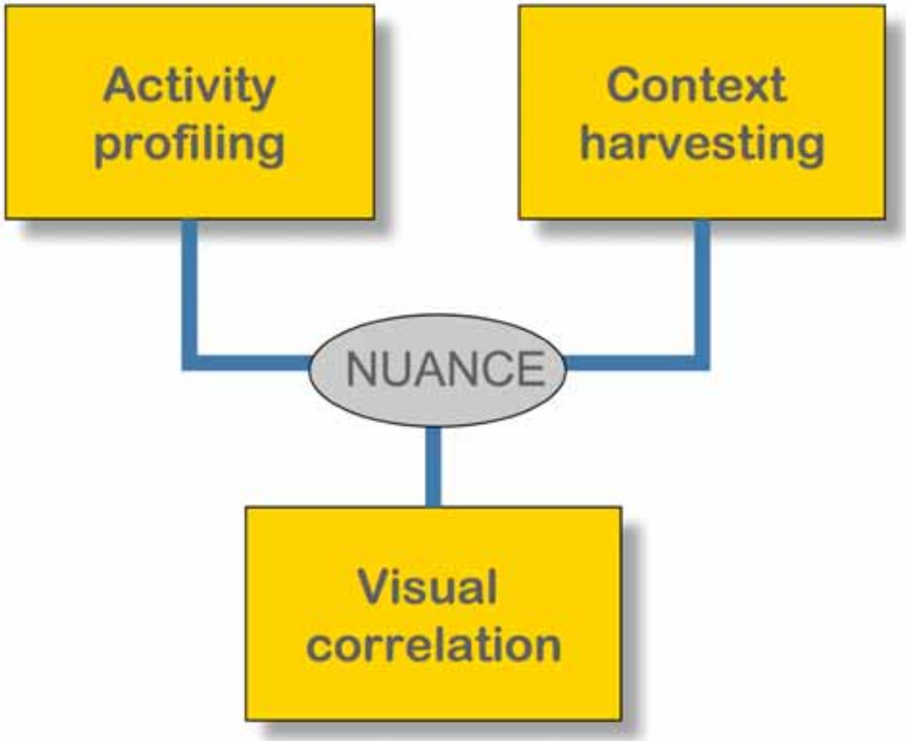
Cyber data

Malicious activity

Cyber data *plus*…

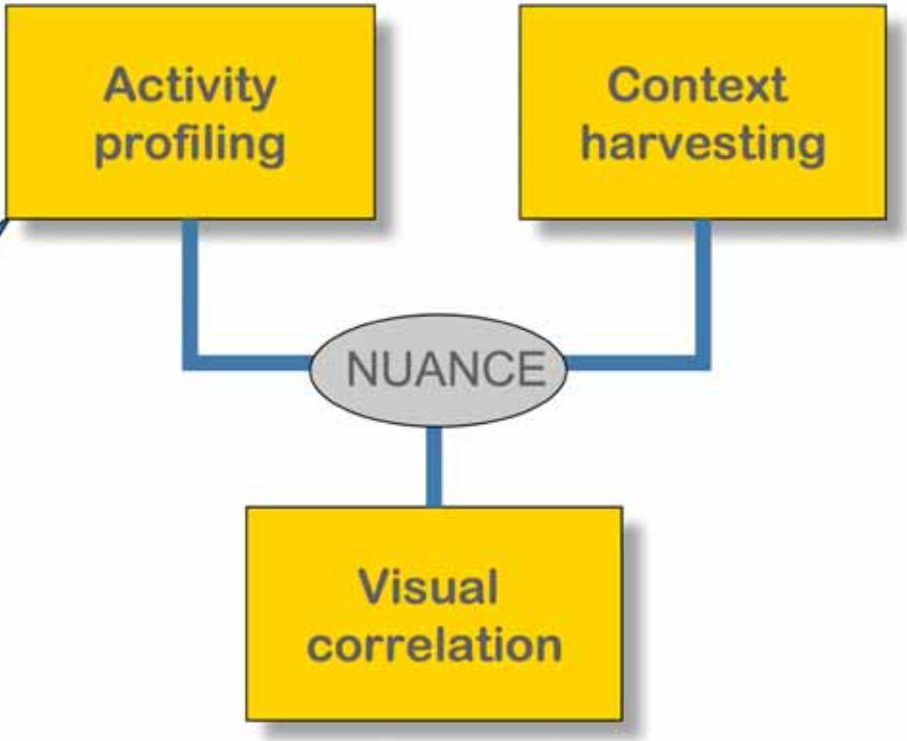
NUANCE

The NUANCE Approach

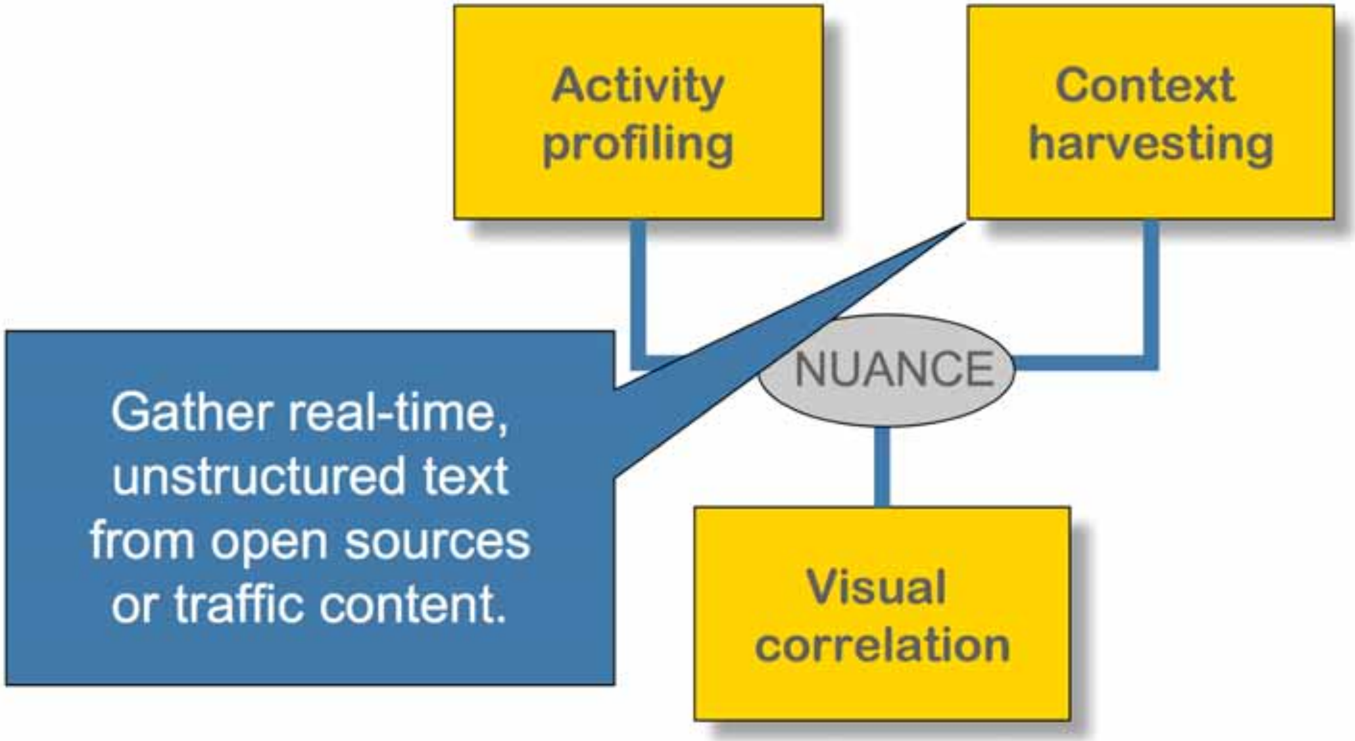


The NUANCE Approach

Model multi-timescale baseline behaviors for massive numbers of actors (IP addresses) and groups (organization, region) on a network.

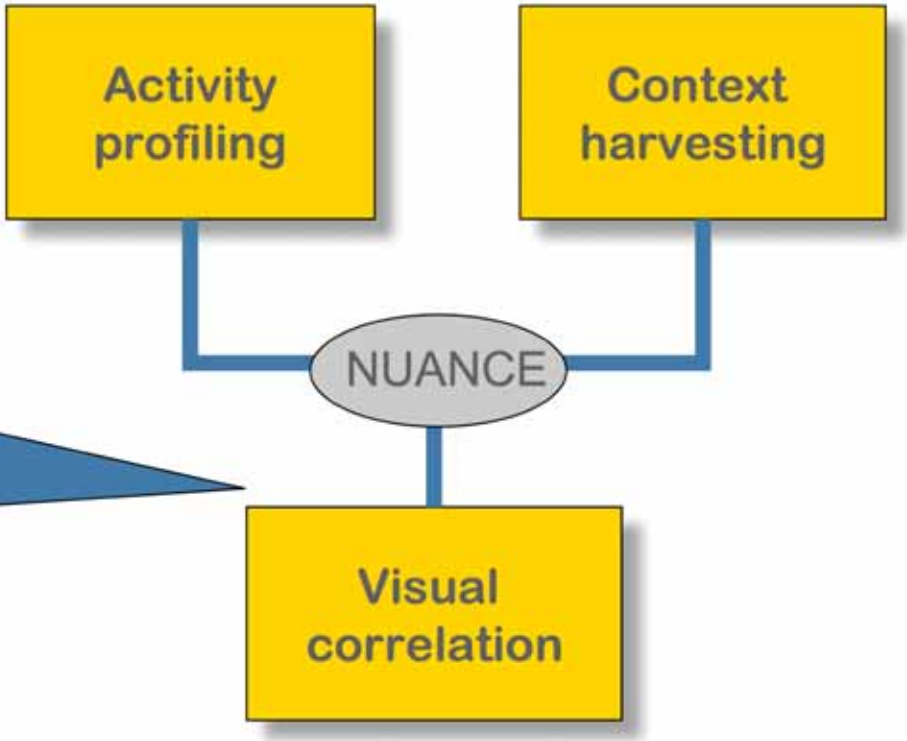


The NUANCE Approach



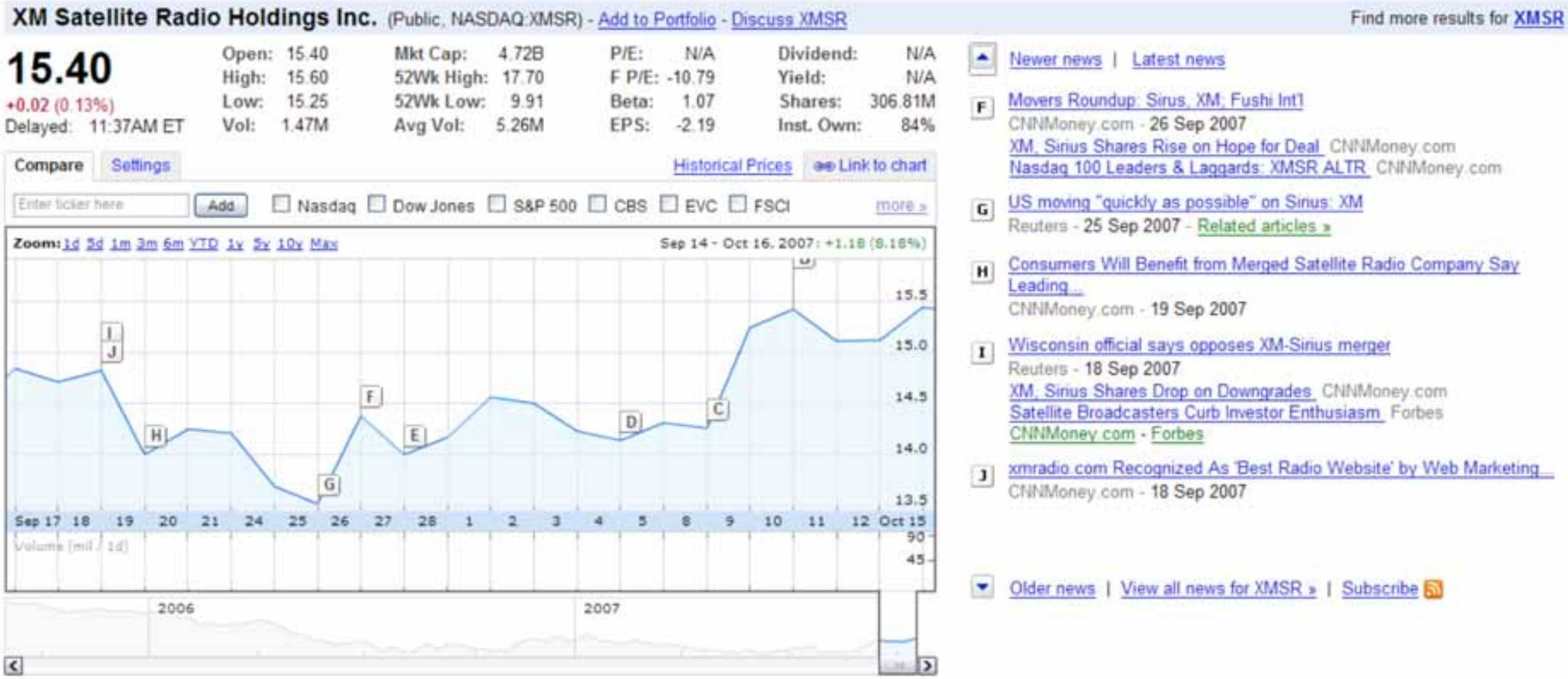
Gather real-time, unstructured text from open sources or traffic content.

The NUANCE Approach



Correlate activity signatures with context signatures, helping analysts identify and explain malicious activities.

Anomaly contextualization analogy



XM Satellite Radio Holdings Inc. (Public, NASDAQ:XMSR) - Add to Portfolio - Discuss XMSR

Find more results for XMSR

15.40
+0.02 (0.13%)
Delayed: 11:37AM ET

Open:	15.40	Mkt Cap:	4.72B	P/E:	N/A	Dividend:	N/A
High:	15.60	52Wk High:	17.70	F P/E:	-10.79	Yield:	N/A
Low:	15.25	52Wk Low:	9.91	Beta:	1.07	Shares:	306.81M
Vol:	1.47M	Avg Vol:	5.26M	EPS:	-2.19	Inst. Own:	84%

Sep 14 - Oct 16, 2007: +1.18 (8.18%)

Compare
Settings
Historical Prices
Link to chart
Enter ticker here
Add
□ Nasdaq □ Dow Jones □ S&P 500 □ CBS □ EVC □ FSCI
more »
Zoom: 1d 5d 1m 3m 6m YTD 1y 5y 10y Max
15.5
15.0
14.5
14.0
13.5
I
J
H
G
F
E
D
C
Sep 17 18 19 20 21 24 25 26 27 28 1 2 3 4 5 8 9 10 11 12 Oct 15
Volume (mil / 1d)
90
45
2006
2007
Newer news | Latest news
Older news | View all news for XMSR » | Subscribe

F Movers Roundup: Sirus, XM; Fushi Int'l
CNNMoney.com - 26 Sep 2007
XM, Sirius Shares Rise on Hope for Deal CNNMoney.com
Nasdaq 100 Leaders & Laggards: XMSR ALTR CNNMoney.com

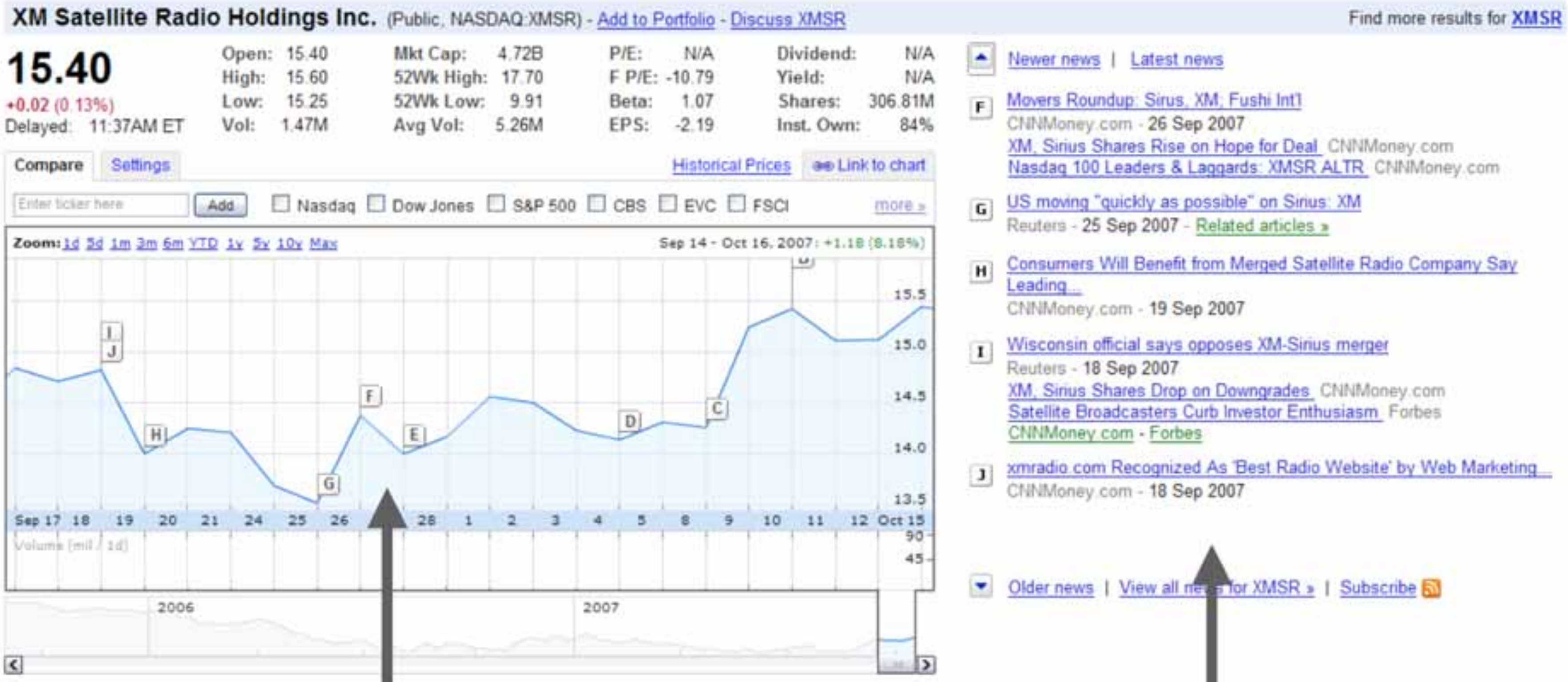
G US moving "quickly as possible" on Sirius: XM
Reuters - 25 Sep 2007 - Related articles »

H Consumers Will Benefit from Merged Satellite Radio Company Say Leading...
CNNMoney.com - 19 Sep 2007

I Wisconsin official says opposes XM-Sirius merger
Reuters - 18 Sep 2007
XM, Sirius Shares Drop on Downgrades CNNMoney.com
Satellite Broadcasters Curb Investor Enthusiasm Forbes
CNNMoney.com - Forbes

J xmradio.com Recognized As 'Best Radio Website' by Web Marketing...
CNNMoney.com - 18 Sep 2007

Anomaly contextualization analog



XM Satellite Radio Holdings Inc. (Public, NASDAQ:XMSR) - Add to Portfolio - Discuss XMSR

Find more results for **XMSR**

15.40
+0.02 (0.13%)
Delayed: 11:37AM ET

Open:	15.40	Mkt Cap:	4.72B	P/E:	N/A	Dividend:	N/A
High:	15.60	52Wk High:	17.70	F P/E:	-10.79	Yield:	N/A
Low:	15.25	52Wk Low:	9.91	Beta:	1.07	Shares:	306.81M
Vol:	1.47M	Avg Vol:	5.26M	EPS:	-2.19	Inst. Own:	84%

Compare
Settings
Historical Prices
Link to chart
Enter ticker here
Add
□ Nasdaq □ Dow Jones □ S&P 500 □ CBS □ EVC □ FSCI
more »
Zoom: 1d 5d 1m 3m 6m YTD 1y 5y 10y Max
Sep 14 - Oct 16, 2007: +1.18 (8.18%)
15.5
15.0
14.5
14.0
13.5
I
J
H
G
F
E
D
C
B
Sep 17 18 19 20 21 24 25 26 28 1 2 3 4 5 8 9 10 11 12 Oct 15
Volume (mil / 1d)
90
45
2006
2007

Newer news | Latest news

F Movers Roundup: Sirus, XM; Fushi Int'l
CNNMoney.com - 26 Sep 2007
XM, Sirius Shares Rise on Hope for Deal CNNMoney.com
Nasdaq 100 Leaders & Laggards: XMSR ALTR CNNMoney.com

G US moving "quickly as possible" on Sirius: XM
Reuters - 25 Sep 2007 - Related articles »

H Consumers Will Benefit from Merged Satellite Radio Company Say Leading...
CNNMoney.com - 19 Sep 2007

I Wisconsin official says opposes XM-Sirius merger
Reuters - 18 Sep 2007
XM, Sirius Shares Drop on Downgrades CNNMoney.com
Satellite Broadcasters Curb Investor Enthusiasm Forbes
CNNMoney.com - Forbes

J xmradio.com Recognized As 'Best Radio Website' by Web Marketing...
CNNMoney.com - 18 Sep 2007

Older news | View all news for XMSR » | Subscribe

Observed Signal
(Summary of behaviors)

External indicators
and drivers

What do our users want?

What do our users want?

"I just want to know where to focus my time."

What do our users want?

"I just want to know where to focus my time."

"I try to keep on top of the latest vulnerabilities, but it's hard."

What do our users want?

"I just want to know where to focus my time."

"I try to keep on top of the latest vulnerabilities, but it's hard."

"We need to organize our hay into smaller piles."

What do our users want?

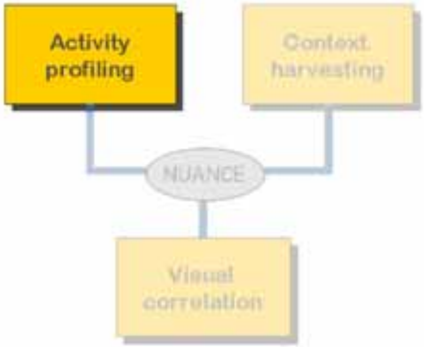
“I just want to know where to focus my time.”

“I try to keep on top of the latest vulnerabilities, but it’s hard.”

“We need to organize our hay into smaller piles.”

“I need to be proactive; forensics is good, but forewarning is better.”

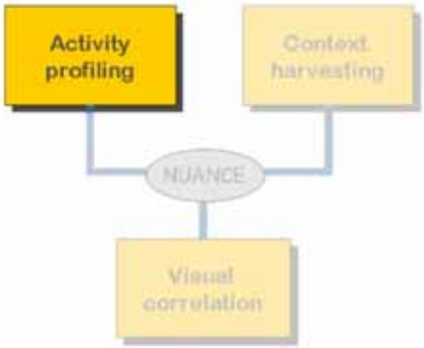
Modeling behavior on a massive scal



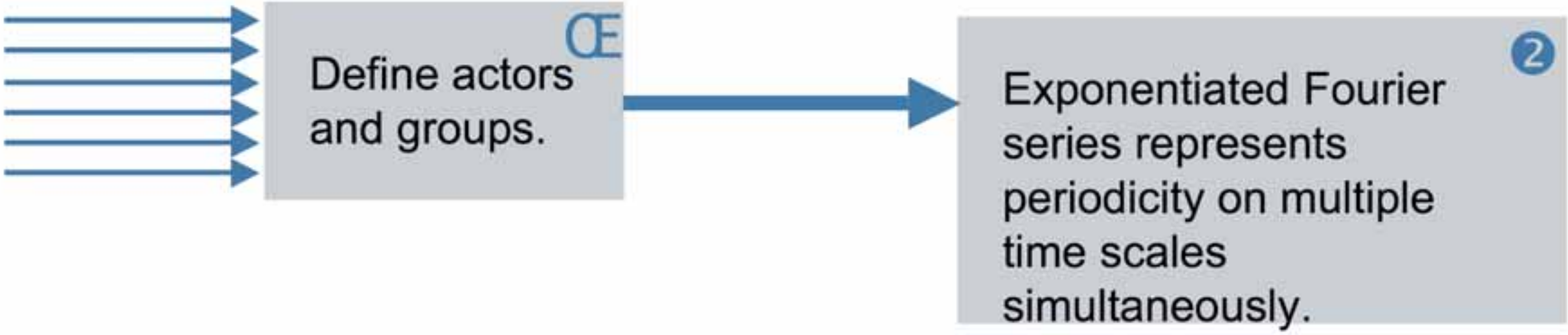
Modeling behavior on a massive scal

Œ

Define actors and groups.

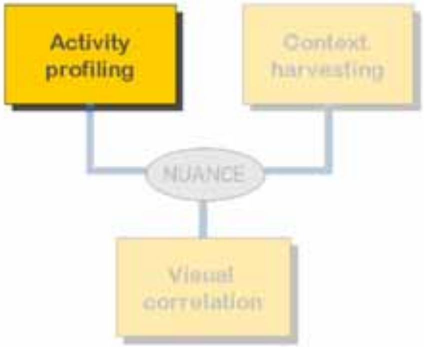


Modeling behavior on a massive scal

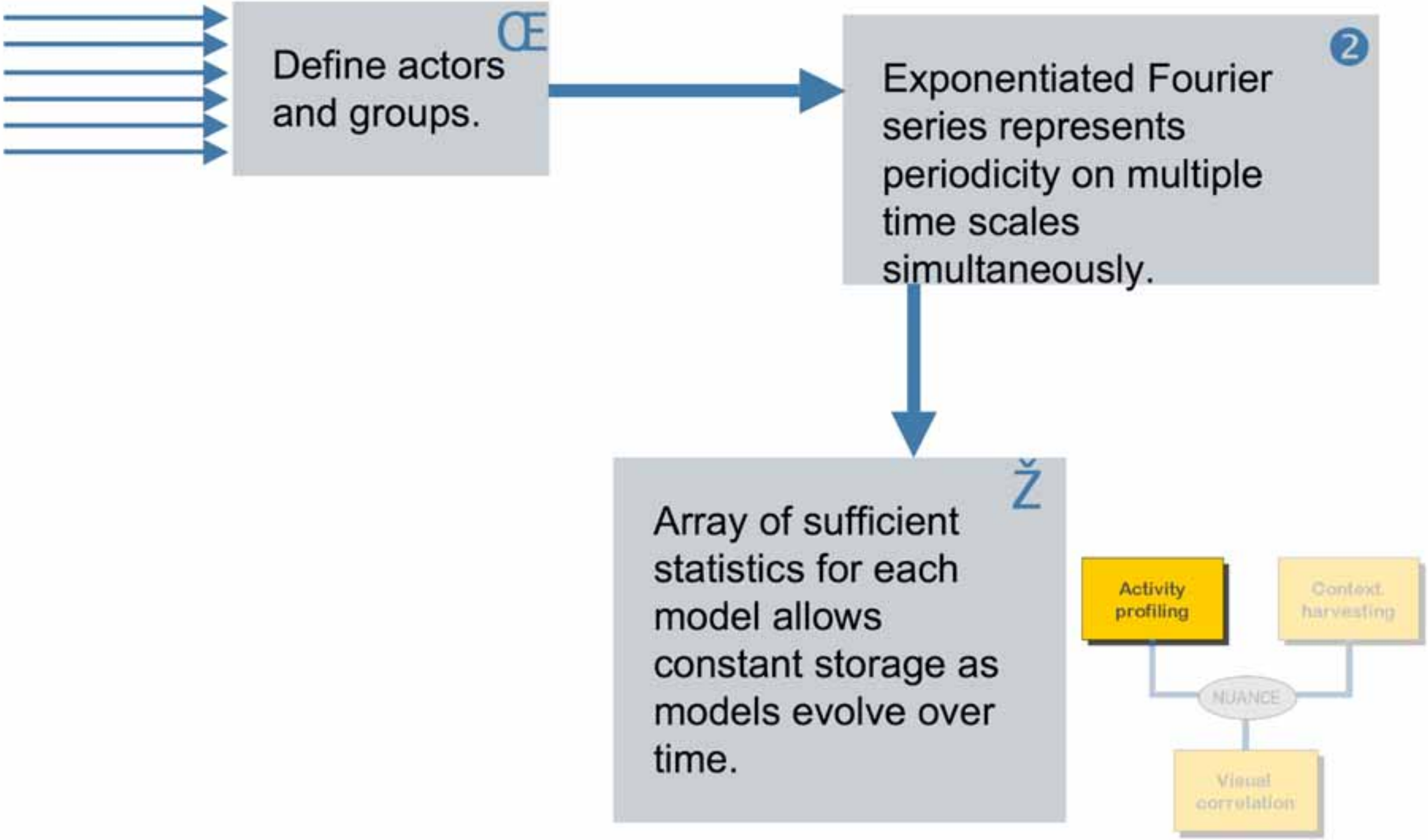


Define actors and groups.

Exponentiated Fourier series represents periodicity on multiple time scales simultaneously.



Modeling behavior on a massive scal

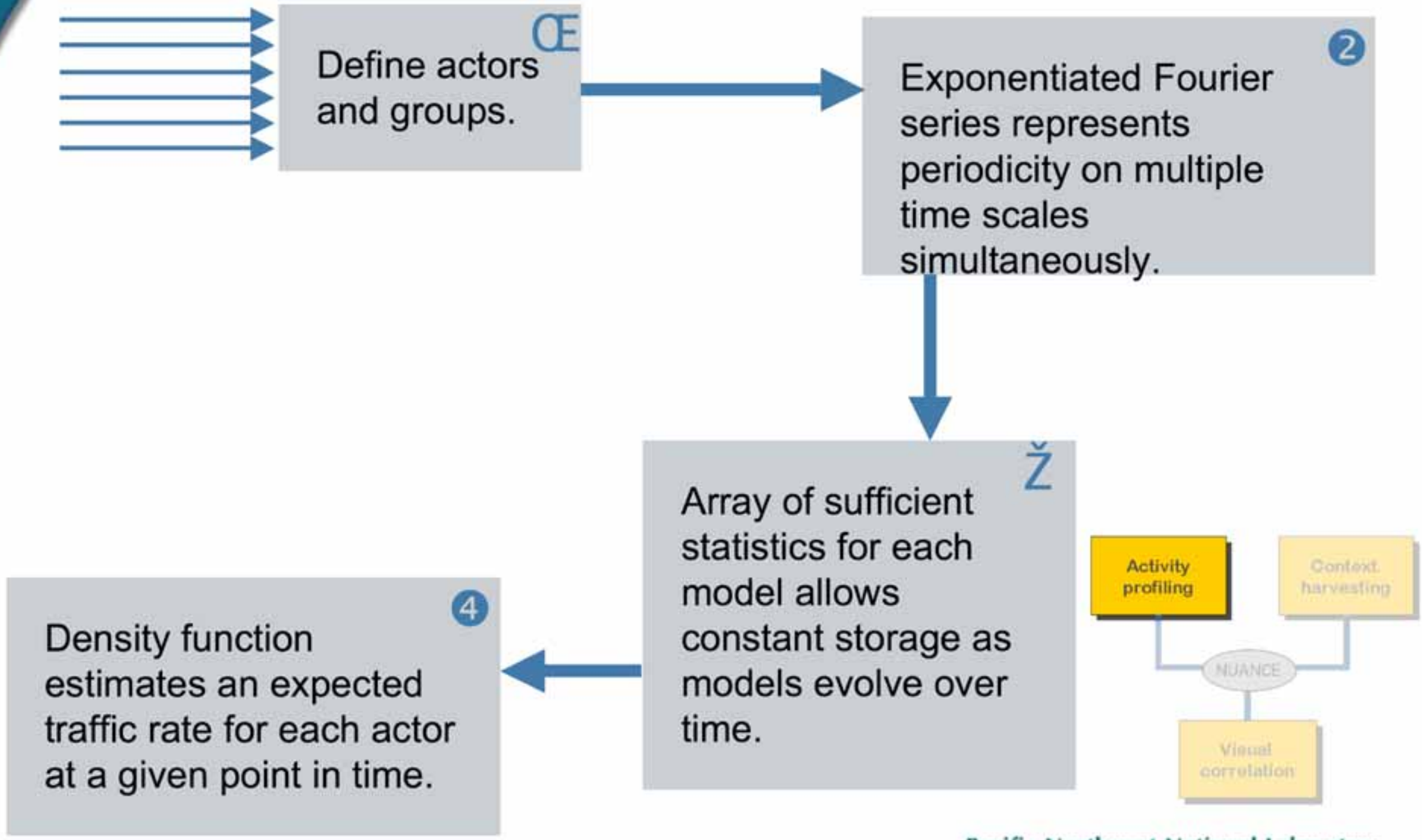


Œ Define actors and groups.

❷ Exponentiated Fourier series represents periodicity on multiple time scales simultaneously.

Ž Array of sufficient statistics for each model allows constant storage as models evolve over time.

Modeling behavior on a massive scal



Œ Define actors and groups.

2 Exponentiated Fourier series represents periodicity on multiple time scales simultaneously.

Ž Array of sufficient statistics for each model allows constant storage as models evolve over time.

4 Density function estimates an expected traffic rate for each actor at a given point in time.

Modeling behavior on a massive scal

Œ

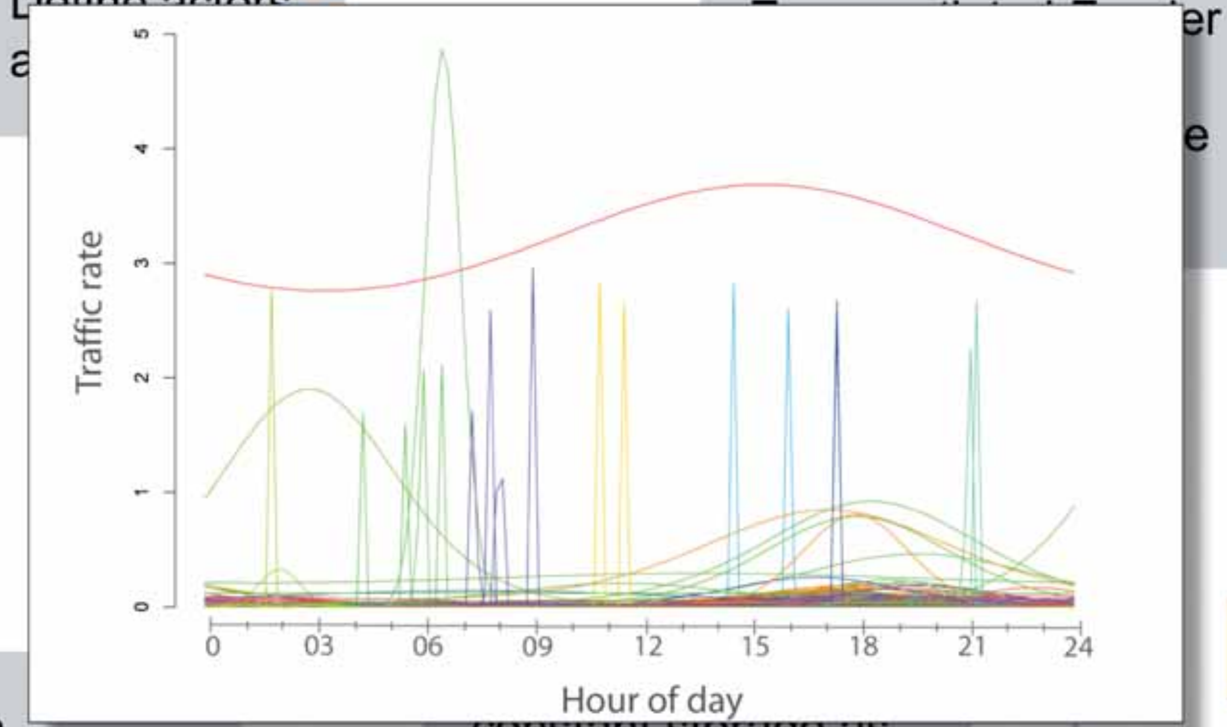
Define actors

a

❷

er

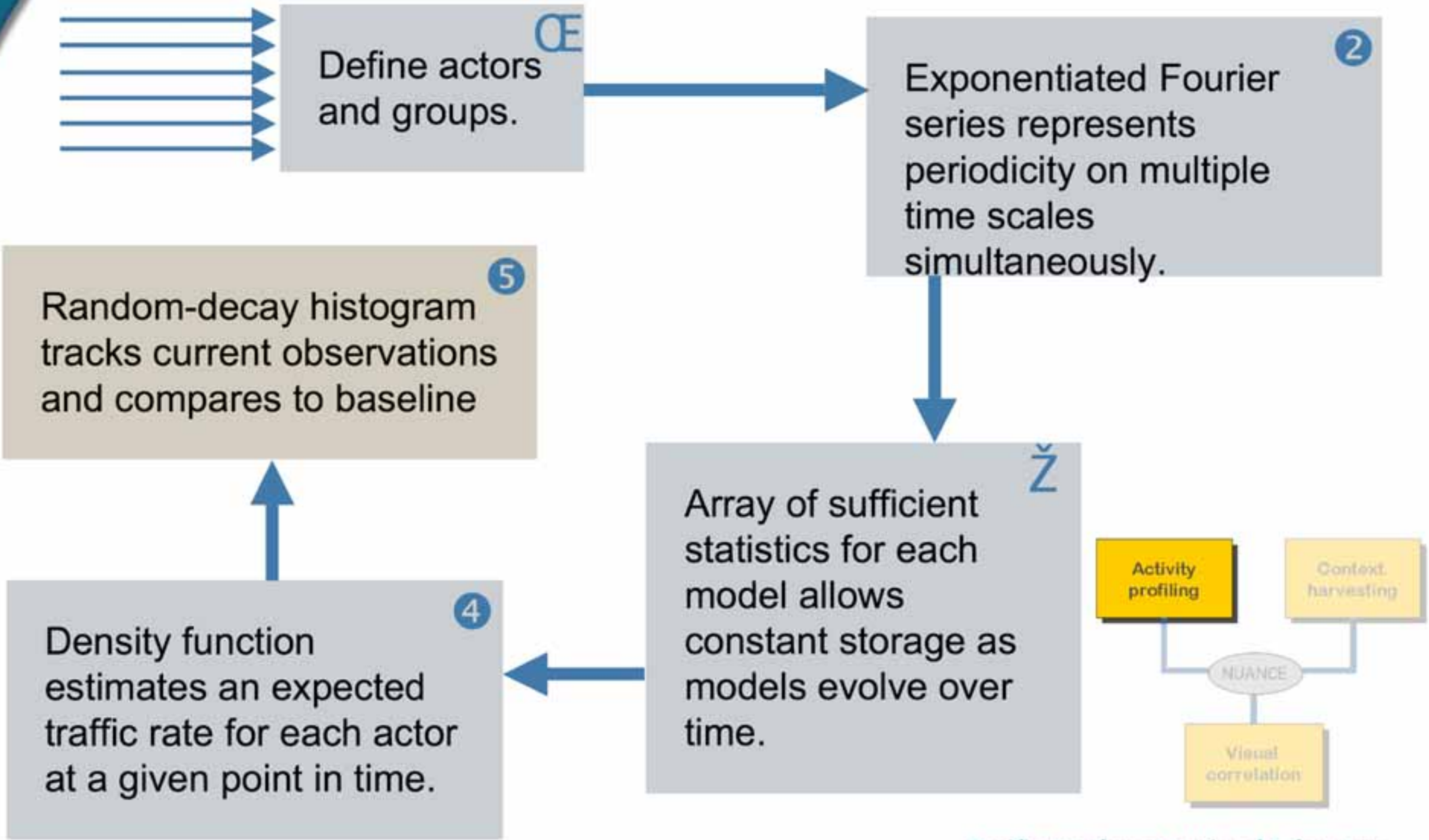
e



Density function estimates an expected traffic rate for each actor at a given point in time.

constant storage as models evolve over time.

Modeling behavior on a massive scal



Œ Define actors and groups.

2 Exponentiated Fourier series represents periodicity on multiple time scales simultaneously.

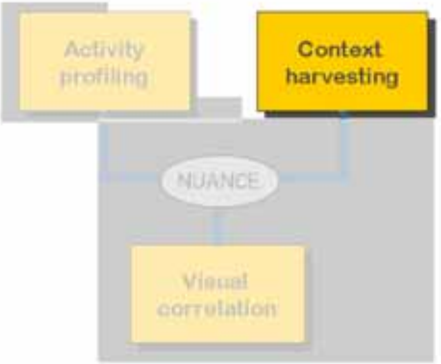
Ž Array of sufficient statistics for each model allows constant storage as models evolve over time.

4 Density function estimates an expected traffic rate for each actor at a given point in time.

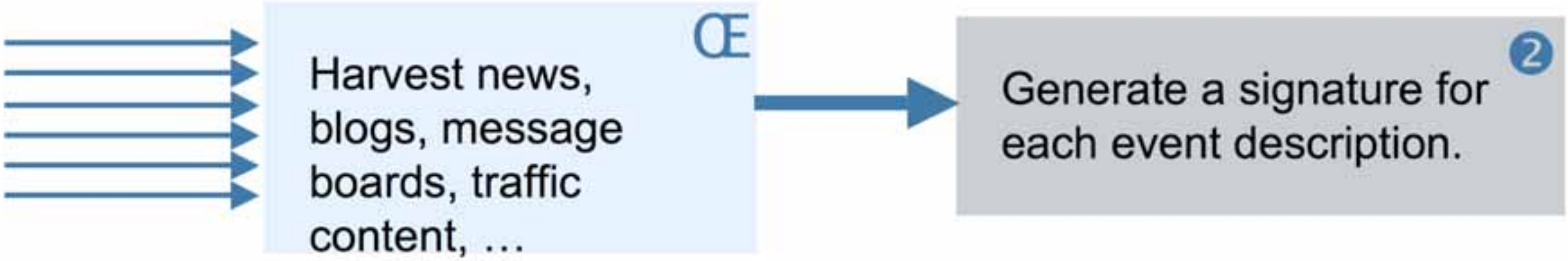
5 Random-decay histogram tracks current observations and compares to baseline

Putting behavior in context

Harvest news, blogs, message boards, traffic content, …



Putting behavior in context

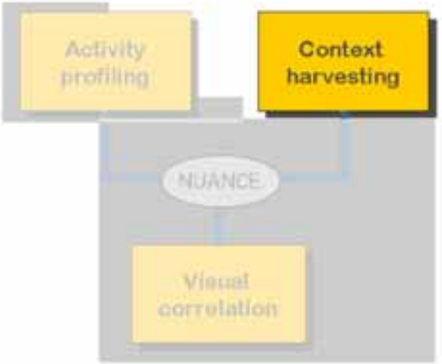


Œ

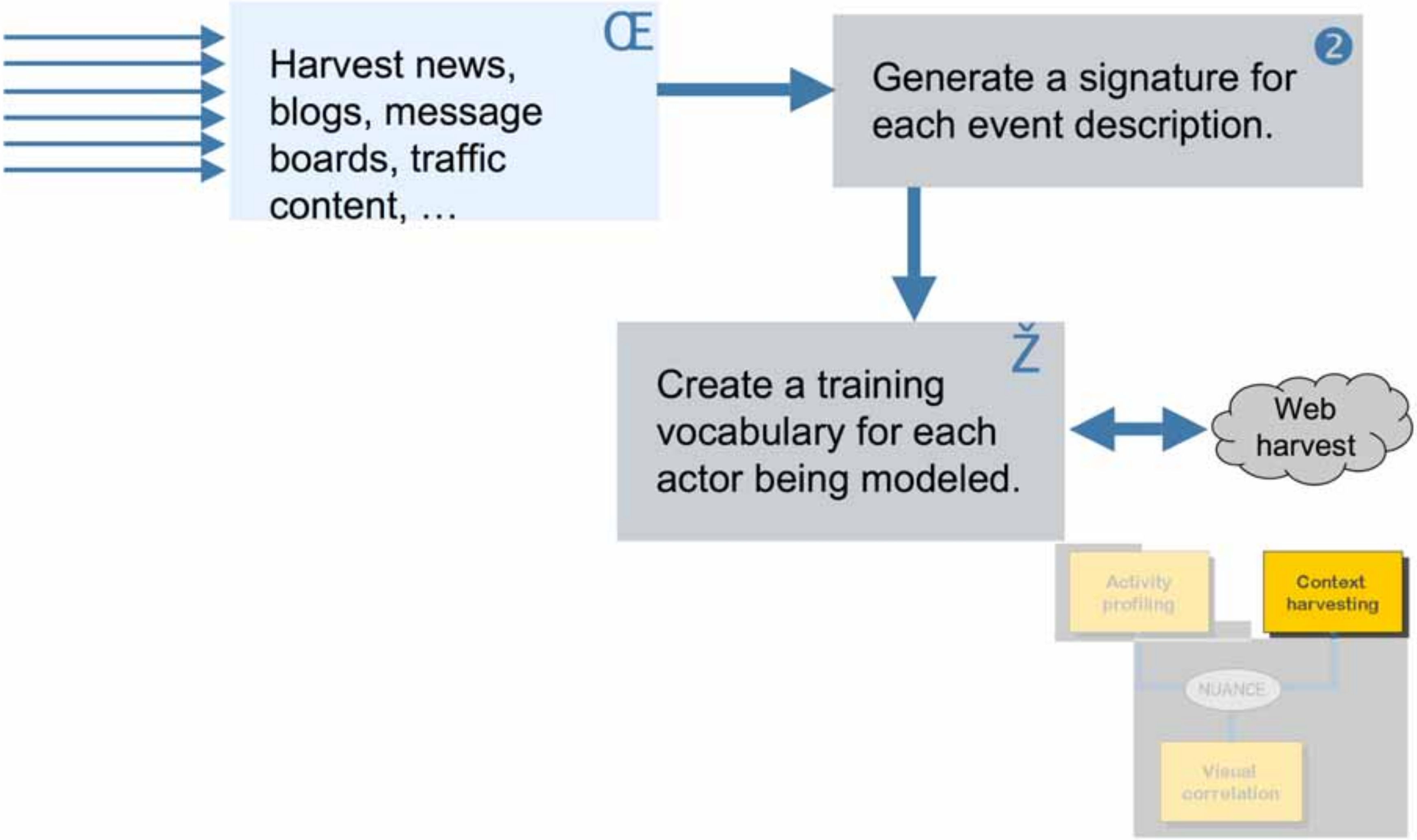
Harvest news, blogs, message boards, traffic content, …

②

Generate a signature for each event description.



Putting behavior in context

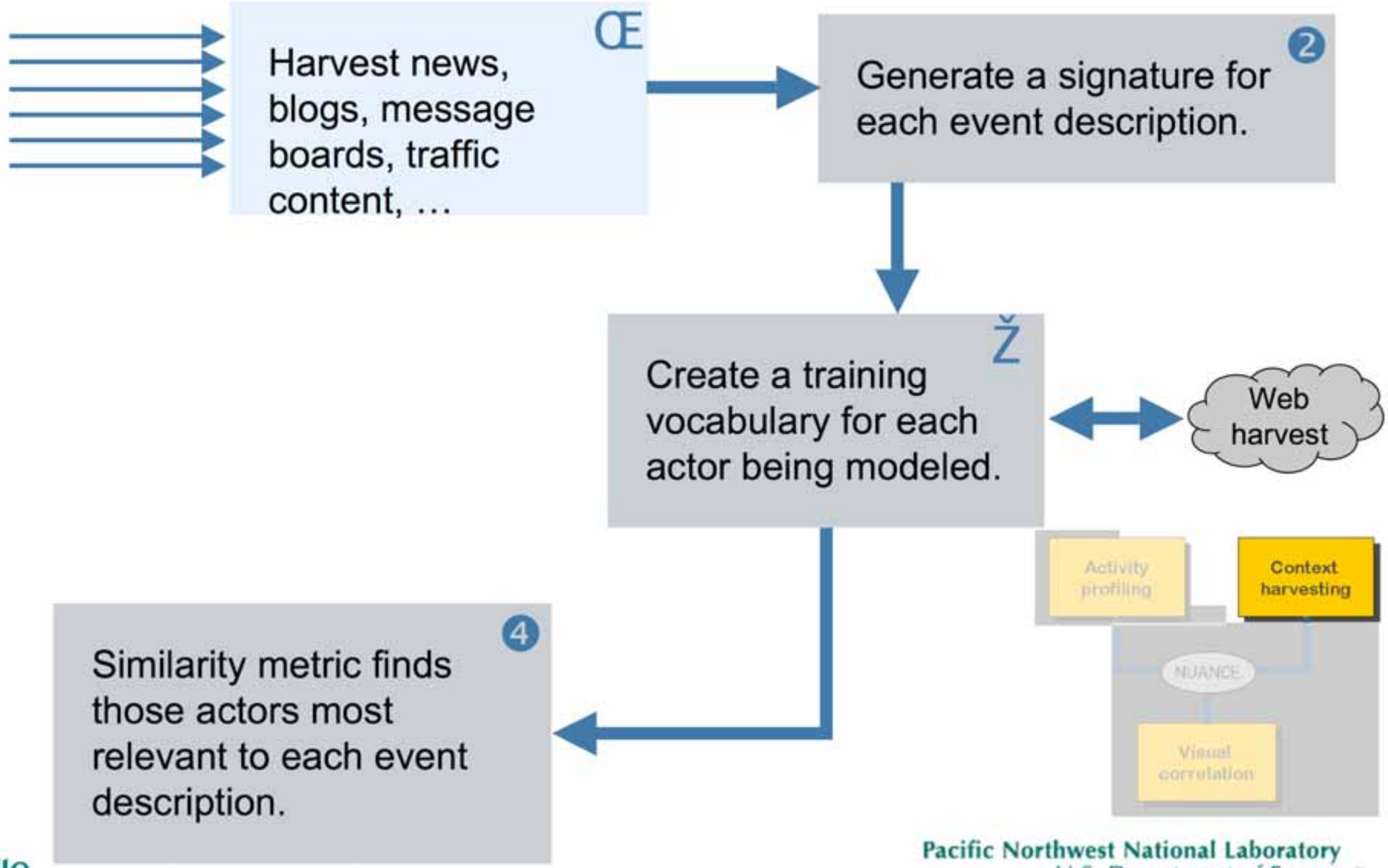


Œ Harvest news, blogs, message boards, traffic content, …

❷ Generate a signature for each event description.

Ž Create a training vocabulary for each actor being modeled.

Putting behavior in context



Œ Harvest news, blogs, message boards, traffic content, …

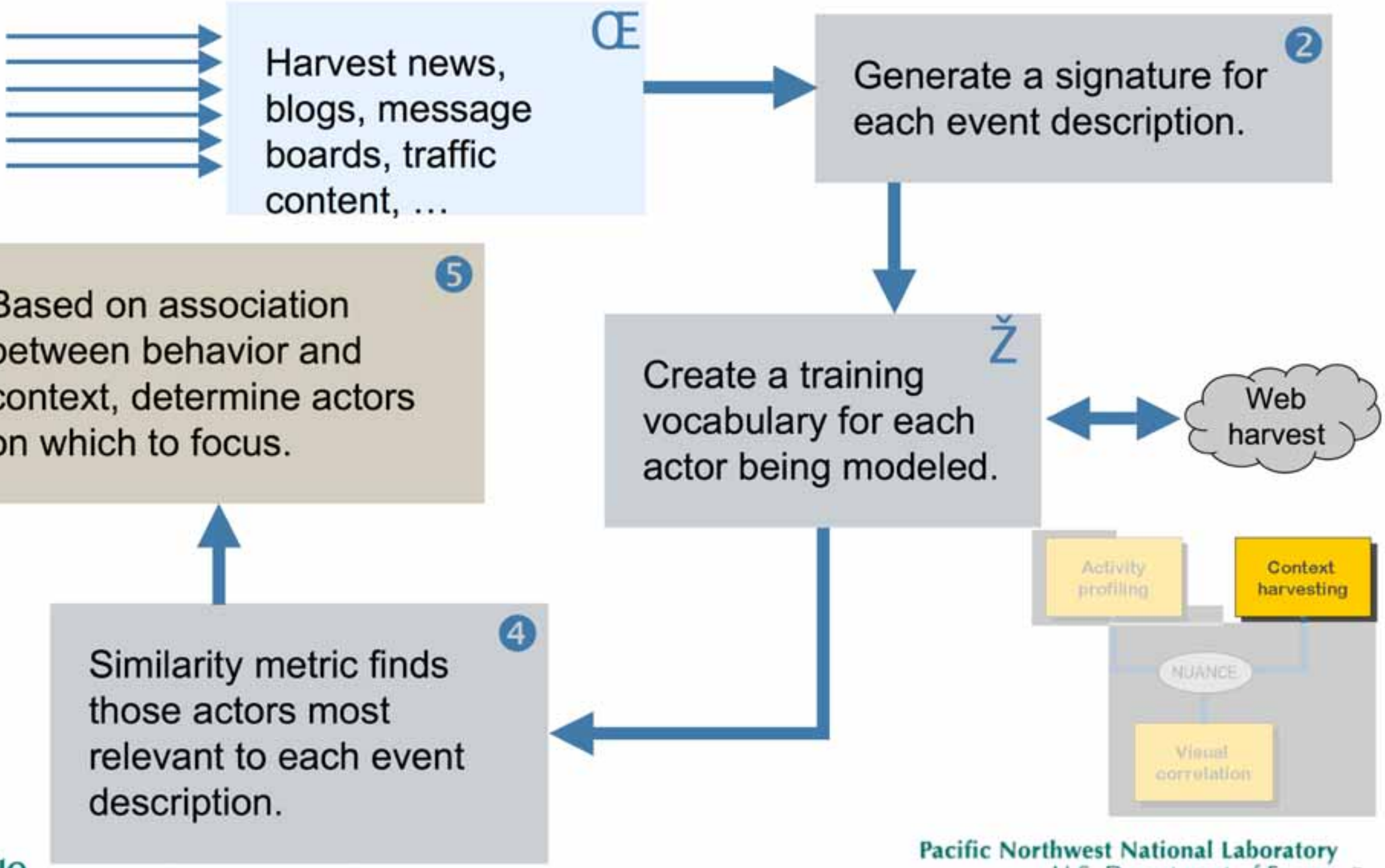
2 Generate a signature for each event description.

Ž Create a training vocabulary for each actor being modeled.

Web harvest

4 Similarity metric finds those actors most relevant to each event description.

Putting behavior in context



Œ Harvest news, blogs, message boards, traffic content, …

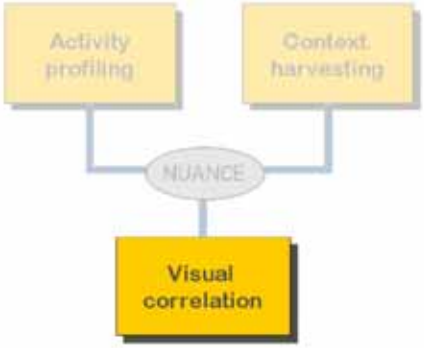
2 Generate a signature for each event description.

Ž Create a training vocabulary for each actor being modeled.

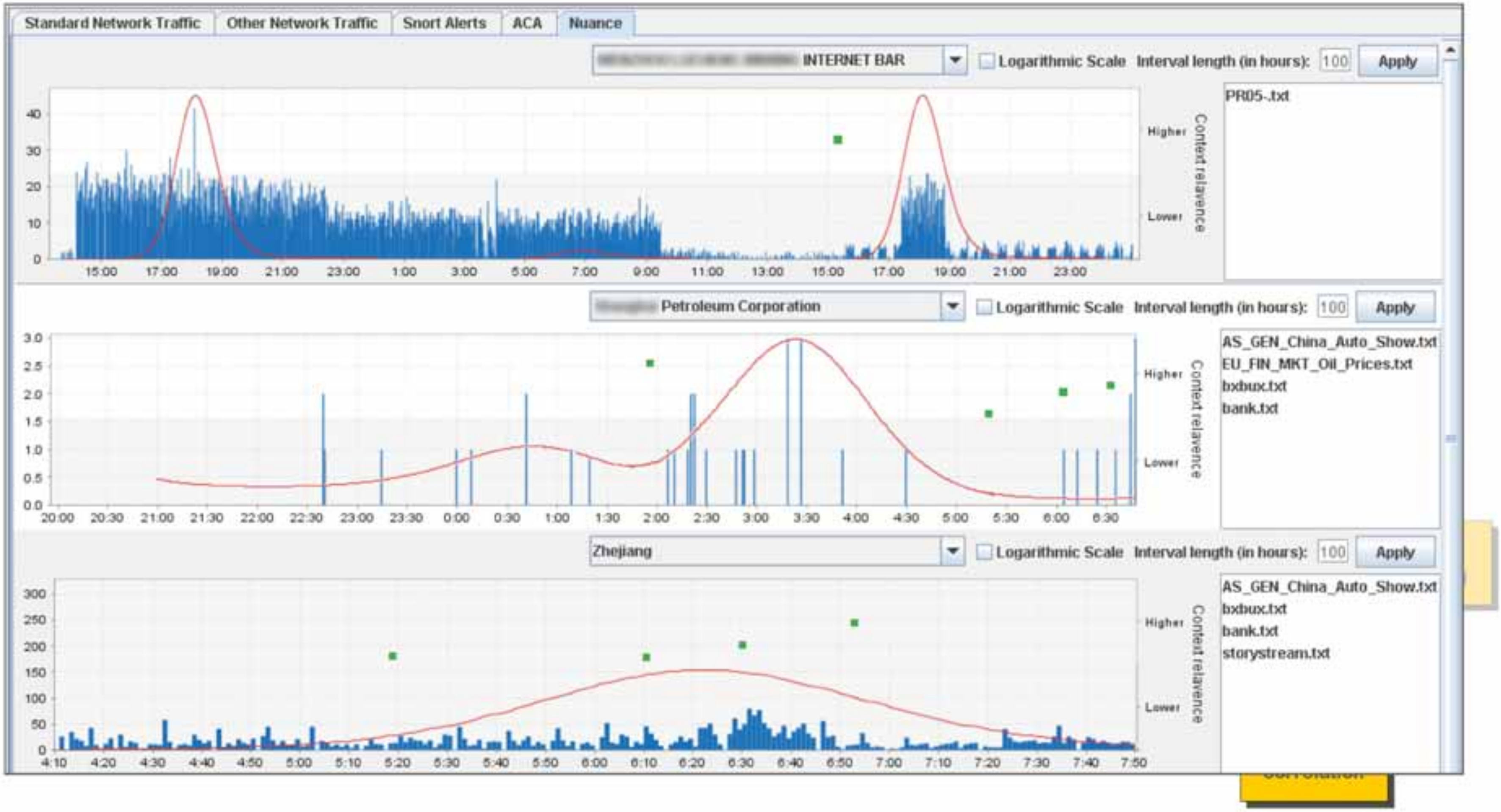
4 Similarity metric finds those actors most relevant to each event description.

5 Based on association between behavior and context, determine actors on which to focus.

Visually fusing behavior and context



Visually fusing behavior and context



[redacted] INTERNET BAR ▾ □ Logarithmic Scale Interval length (in hours): 100

PR05-.txt

[redacted] Petroleum Corporation ▾ □ Logarithmic Scale Interval length (in hours): 100

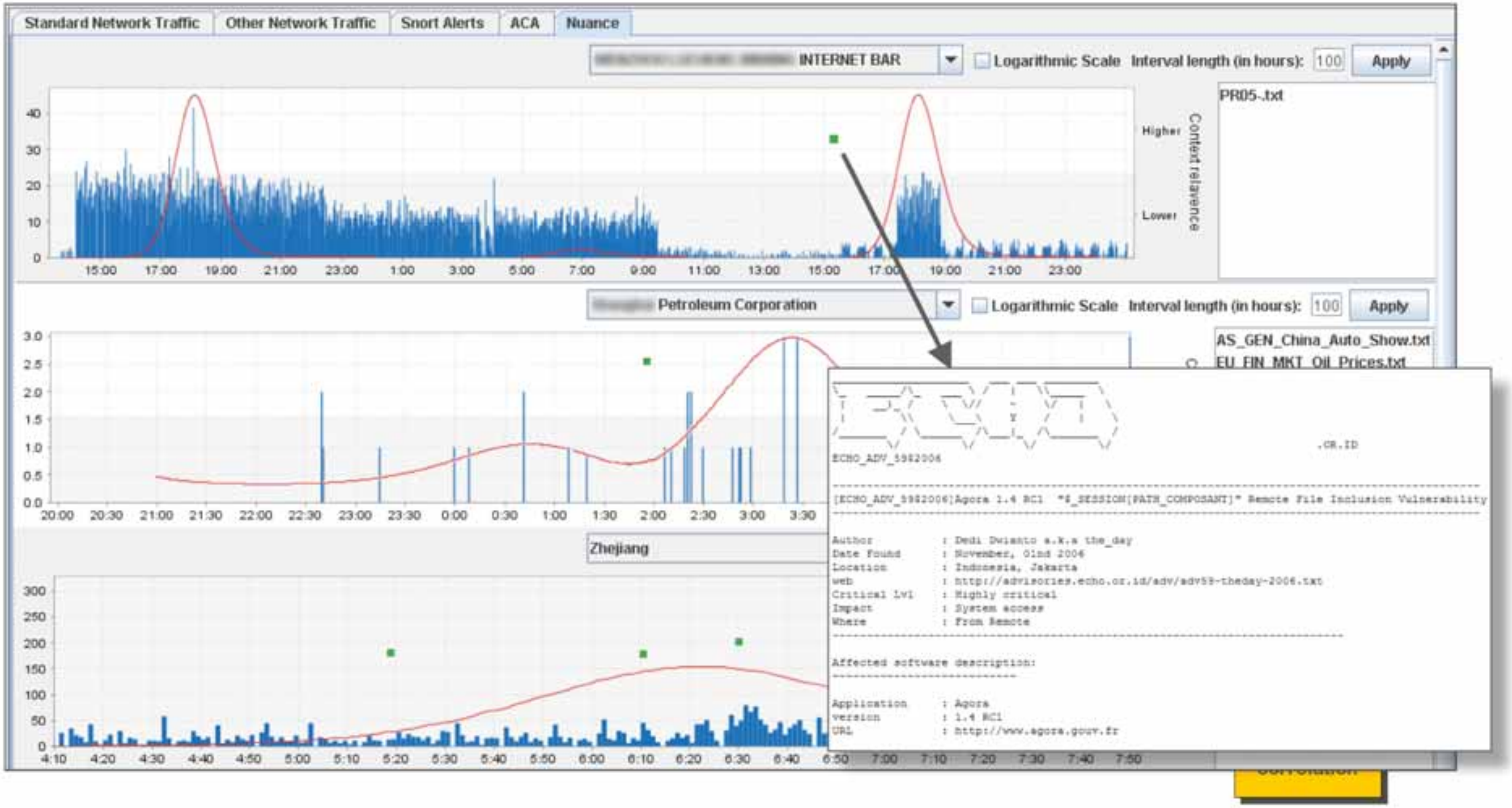
AS_GEN_China_Auto_Show.txt
EU_FIN_MKT_Oil_Prices.txt
bxbux.txt
bank.txt

Zhejiang ▾ □ Logarithmic Scale Interval length (in hours): 100

AS_GEN_China_Auto_Show.txt
bxbux.txt
bank.txt
storystream.txt

Battelle

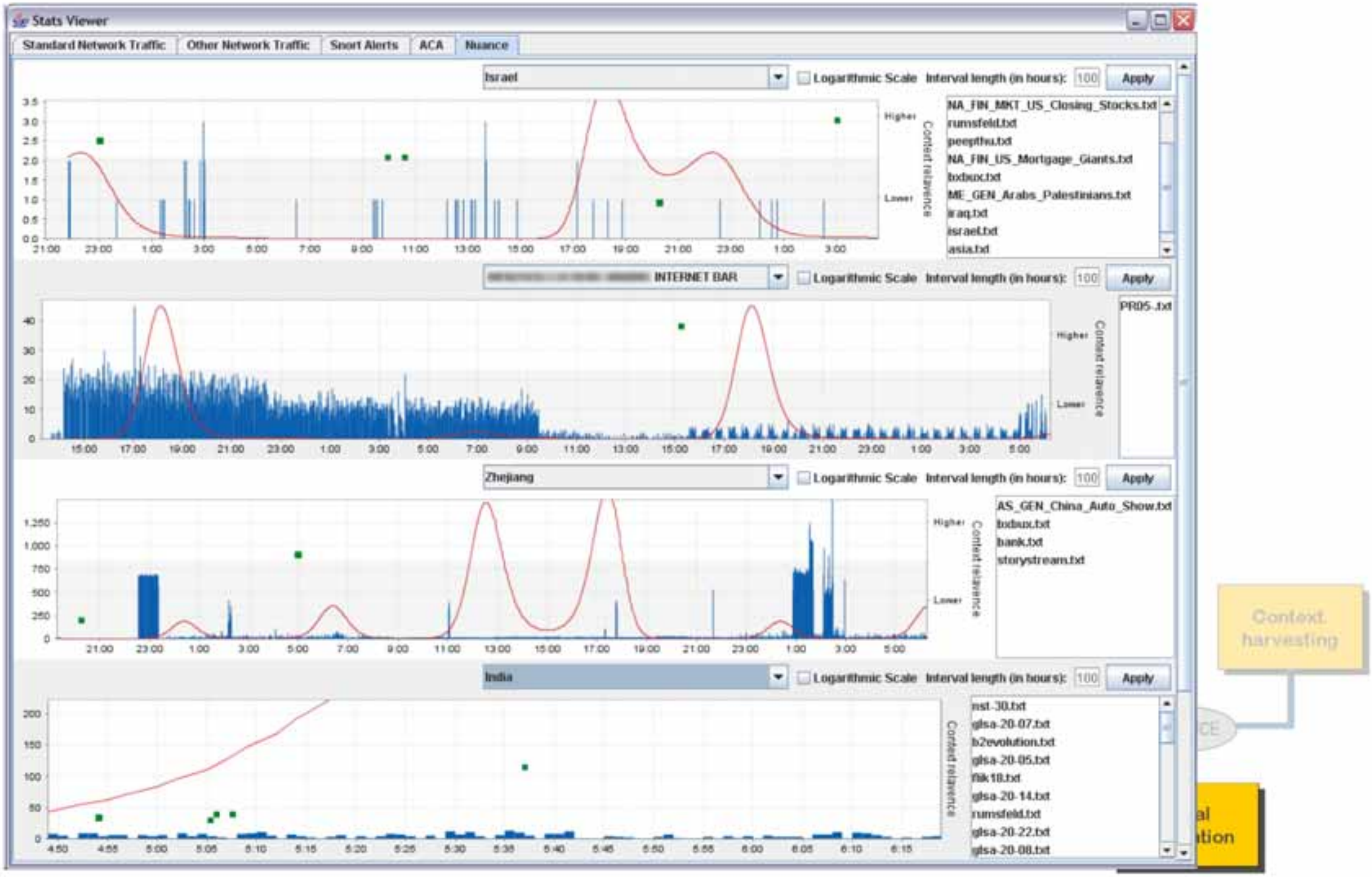
Visually fusing behavior and context



```
                                                                  .OR.ID
ECHO_ADV_5982006

--------------------------------------------------------------------------------
[ECHO_ADV_5982006]Agora 1.4 RC1  "$_SESSION[PATH_COMPOSANT]" Remote File Inclusion Vulnerability
--------------------------------------------------------------------------------

Author          : Dedi Dwianto a.k.a the_day
Date Found      : November, 02nd 2006
Location        : Indonesia, Jakarta
web             : http://advisories.echo.or.id/adv/adv59-theday-2006.txt
Critical Lvl    : Highly critical
Impact          : System access
Where           : From Remote
---------------------------------------------------------------------------

Affected software description:
---------------------------

Application     : Agora
version         : 1.4 RC1
URL             : http://www.agora.gouv.fr
```

Battelle

Visually fusing behavior and context



Stats Viewer

Standard Network Traffic | Other Network Traffic | Snort Alerts | ACA | Nuance

Israel ▾ □ Logarithmic Scale Interval length (in hours): 100 Apply

- NA_FIN_MKT_US_Closing_Stocks.txt
- rumsfeld.txt
- peepthu.txt
- NA_FIN_US_Mortgage_Giants.txt
- txtbux.txt
- ME_GEN_Arabs_Palestinians.txt
- iraq.txt
- israel.txt
- asia.txt

[redacted] INTERNET BAR ▾ □ Logarithmic Scale Interval length (in hours): 100 Apply

- PR05-.txt

Zhejiang ▾ □ Logarithmic Scale Interval length (in hours): 100 Apply

- AS_GEN_China_Auto_Show.txt
- txtbux.txt
- bank.txt
- storystream.txt

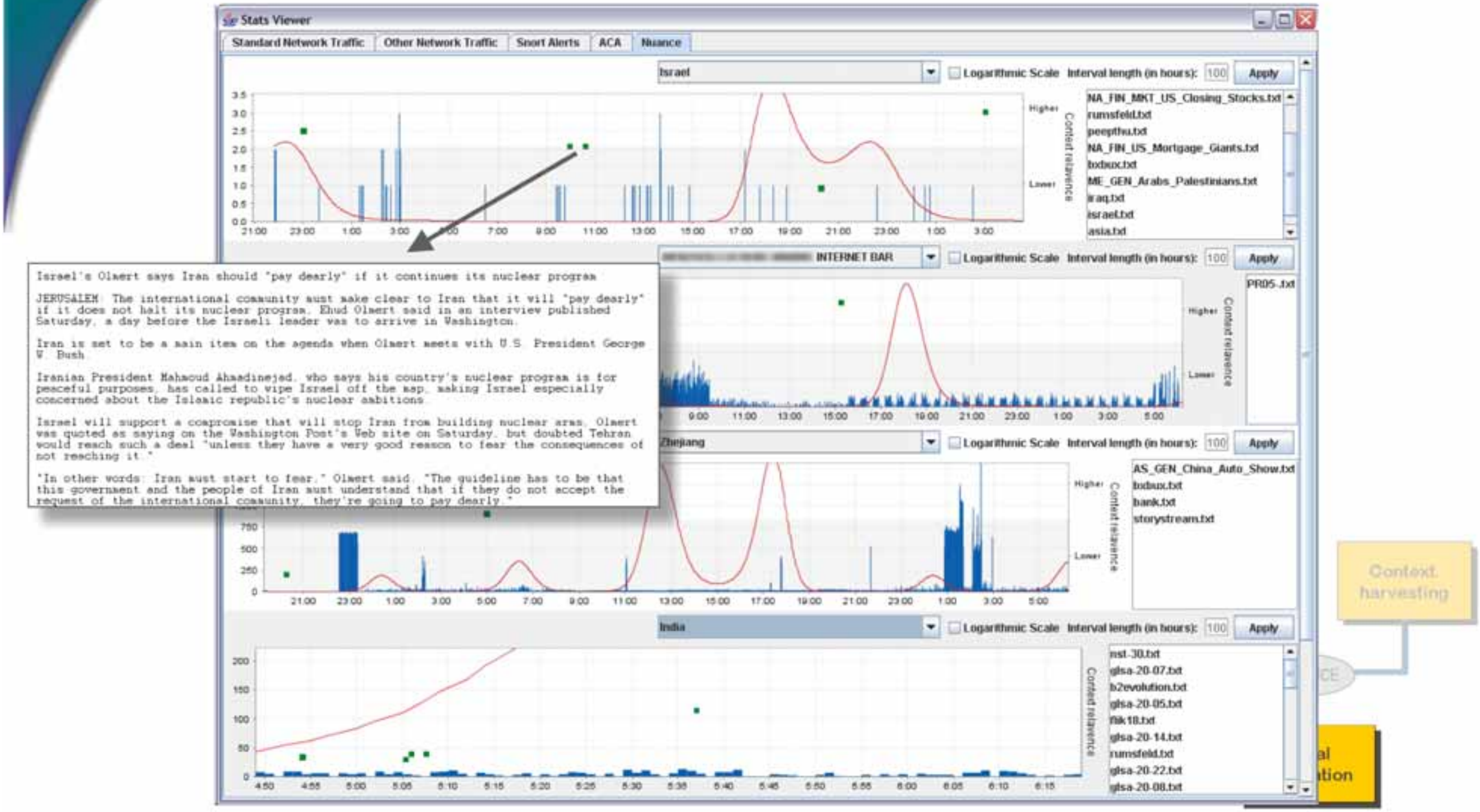
India ▾ □ Logarithmic Scale Interval length (in hours): 100 Apply

- nst-30.txt
- glsa-20-07.txt
- b2evolution.txt
- glsa-20-05.txt
- flik18.txt
- glsa-20-14.txt
- rumsfeld.txt
- glsa-20-22.txt
- glsa-20-08.txt

Battelle

Pacific Northwest National Laboratory
U.S. Department of Energy

Visually fusing behavior and context



Israel's Olmert says Iran should "pay dearly" if it continues its nuclear program

JERUSALEM: The international community must make clear to Iran that it will "pay dearly" if it does not halt its nuclear program, Ehud Olmert said in an interview published Saturday, a day before the Israeli leader was to arrive in Washington.

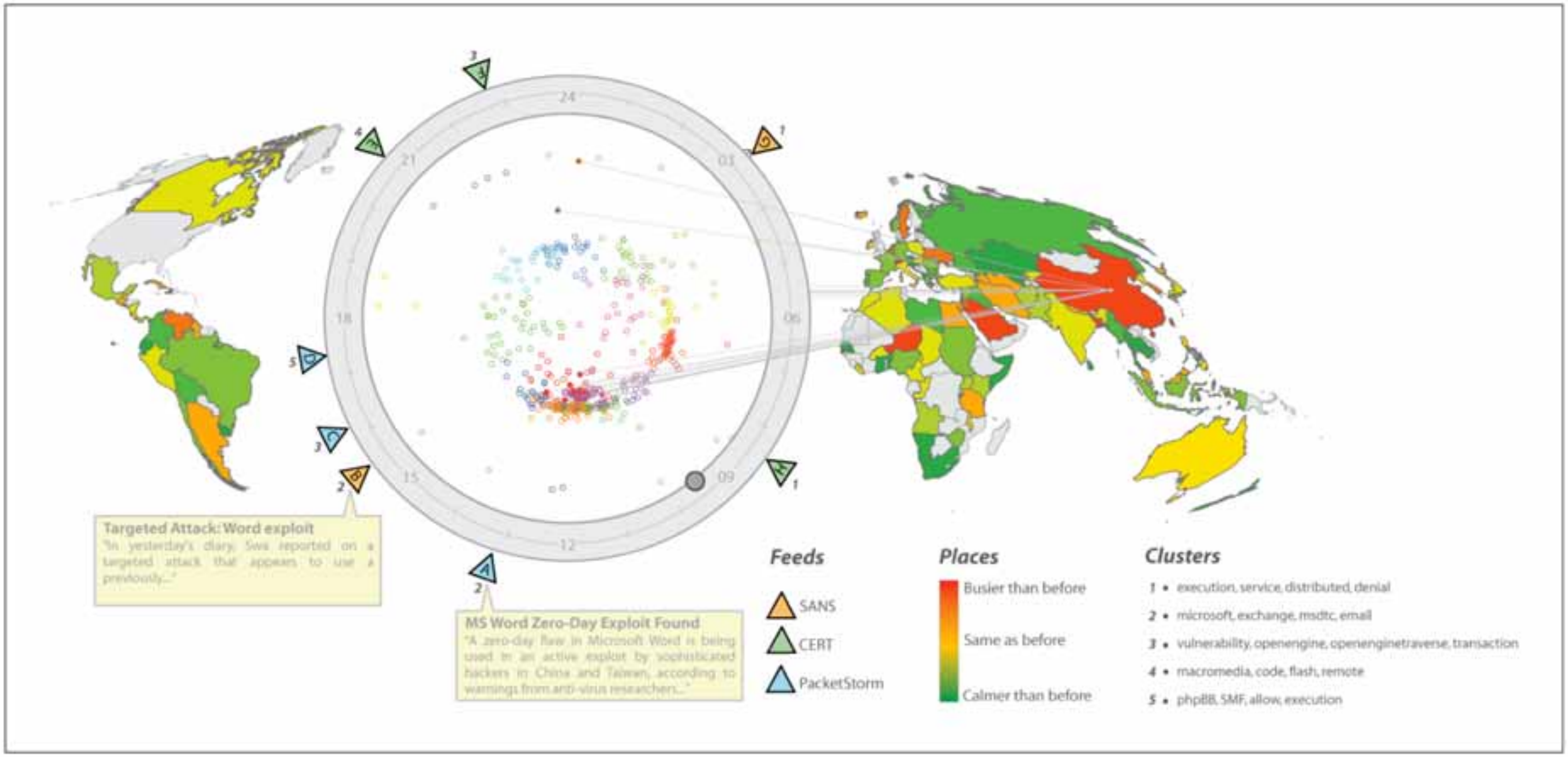
Iran is set to be a main item on the agenda when Olmert meets with U.S. President George W. Bush.

Iranian President Mahmoud Ahmadinejad, who says his country's nuclear program is for peaceful purposes, has called to wipe Israel off the map, making Israel especially concerned about the Islamic republic's nuclear ambitions.

Israel will support a compromise that will stop Iran from building nuclear arms, Olmert was quoted as saying on the Washington Post's Web site on Saturday, but doubted Tehran would reach such a deal "unless they have a very good reason to fear the consequences of not reaching it."

"In other words: Iran must start to fear," Olmert said. "The guideline has to be that this government and the people of Iran must understand that if they do not accept the request of the international community, they're going to pay dearly."

NUANCE monitoring dashboard



24
03
06
09
12
15
18
21
A
B
C
D
F
G
J
1
2
3
4
5
Feeds
SANS
CERT
PacketStorm
Places
Busier than before
Same as before
Calmer than before
Clusters
1 • execution, service, distributed, denial
2 • microsoft, exchange, msdtc, email
3 • vulnerability, openengine, openenginetraverse, transaction
4 • macromedia, code, flash, remote
5 • phpBB, SMF, allow, execution

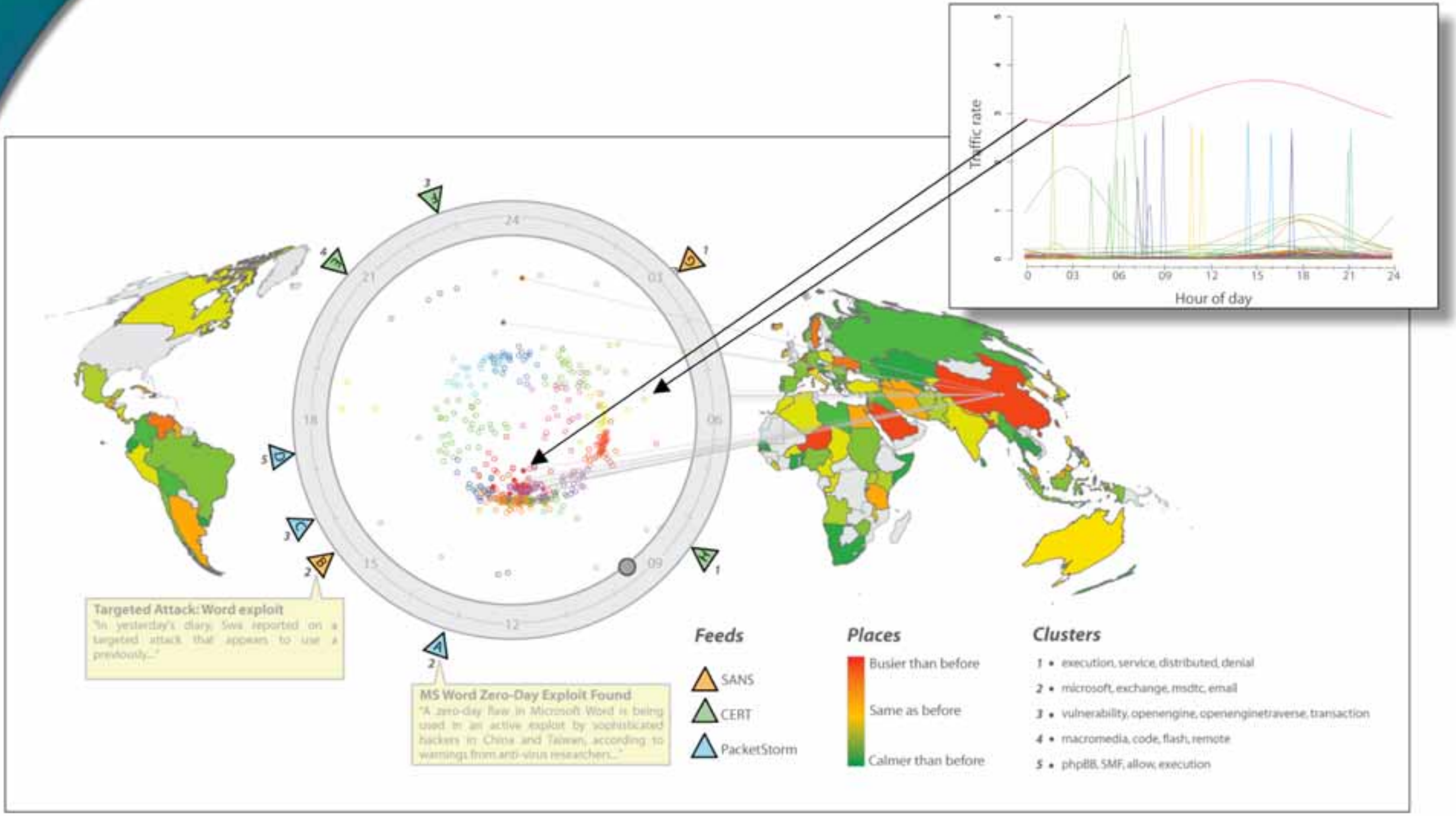
Targeted Attack: Word exploit

"In yesterday's diary, Swa reported on a targeted attack that appears to use a previously..."

MS Word Zero-Day Exploit Found

"A zero-day flaw in Microsoft Word is being used in an active exploit by sophisticated hackers in China and Taiwan, according to warnings from anti-virus researchers..."

NUANCE monitoring dashboard



Traffic rate
Hour of day
0
03
06
09
12
15
18
21
24
24
21
03
18
06
15
09
12
Feeds
SANS
CERT
PacketStorm
Places
Busier than before
Same as before
Calmer than before
Clusters
1 • execution, service, distributed, denial
2 • microsoft, exchange, msdtc, email
3 • vulnerability, openengine, openenginetraverse, transaction
4 • macromedia, code, flash, remote
5 • phpBB, SMF, allow, execution

Targeted Attack: Word exploit

"In yesterday's diary, Swa reported on a targeted attack that appears to use a previously..."

MS Word Zero-Day Exploit Found

"A zero-day flaw in Microsoft Word is being used in an active exploit by sophisticated hackers in China and Taiwan, according to warnings from anti-virus researchers..."

Toward an operational capability

- **Context matters.**
  - Visualizing it helps analysts **explain** events.
- **Parallelization is needed.**
  - NUANCE runs on commodity hardware, but is being scaled to Cray XMT multithreaded architecture.

- **Prediction is the goal.**
  - Nascent behavioral changes can be detected visually in real-time.
  - Historical correlation between activity and context produces indicators for future events.