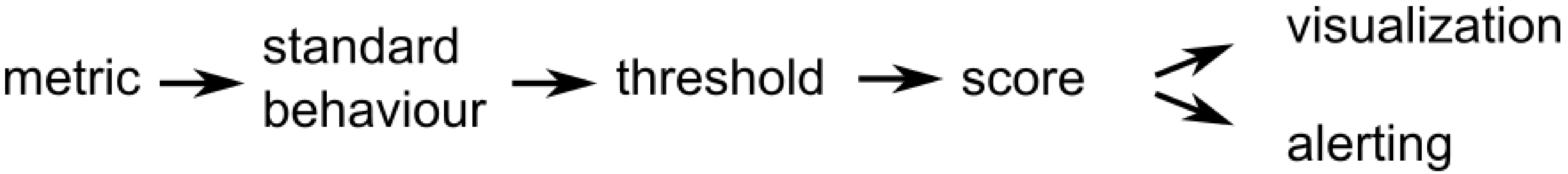
19/10/2017, Usergroup 2017

Next Generation Performance Monitoring
Machine Learning Algorithms for Anomaly Detection

Susanne Greiner

Performance Monitoring

How to monitor performance?

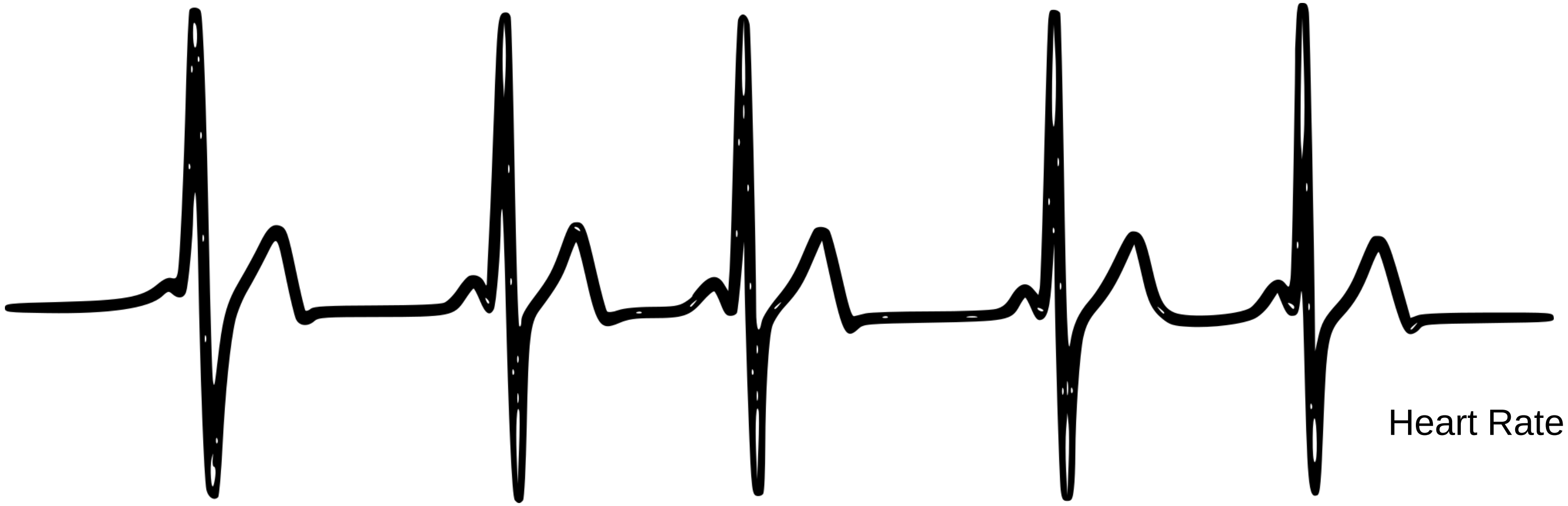


metric → standard behaviour → threshold → score → visualization / alerting

The right decision at each step is not trivial!

Data collection ≠ Problem solution

Performance Monitoring



Can be influenced by

- Pathology
- Sport
- Breathing
- Drugs
- Temperature
- Dehydration
- Pressure
- Etc.

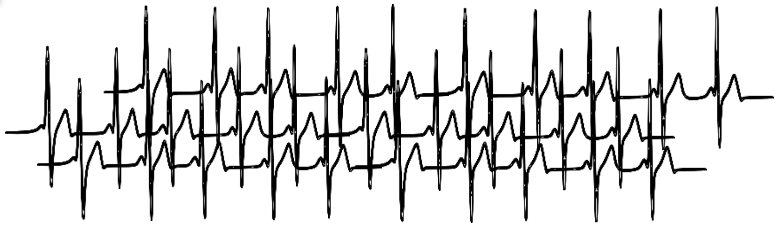
Monitoring & Alarms

Subject specific historical data

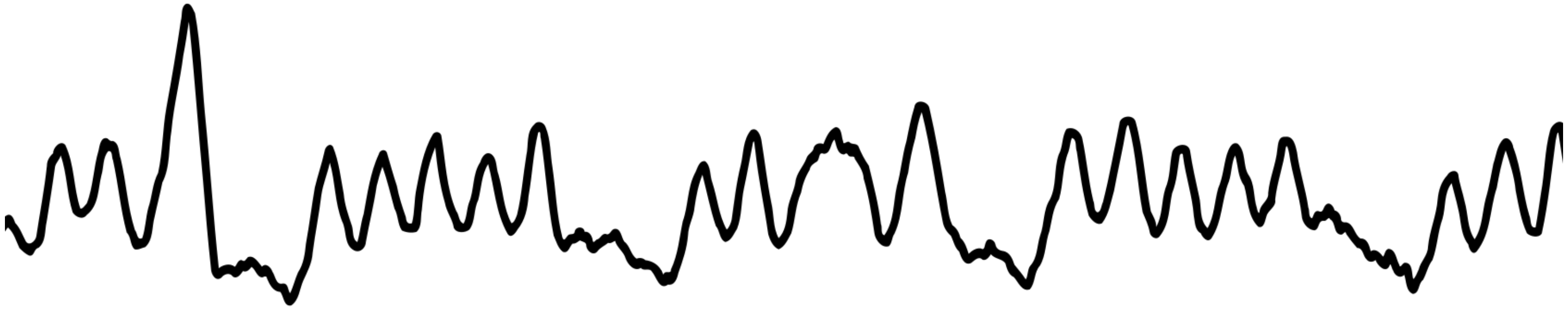
Expectation

- Time series
- Alarm thresholds

Population data



Performance Monitoring



Percentage Processor Time

Can be influenced by

- Batch requests
- Transactions
- Memory
- SAN
- Network
- Side Processes
- Etc.

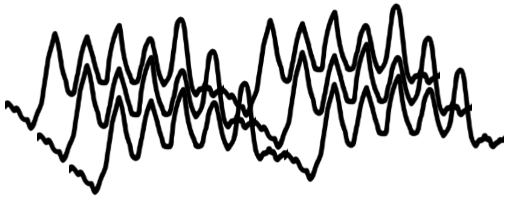
Monitoring & Alarms

Machine/ setting specific historical data

Expectation

- Time series
- Alarm thresholds

Experience,
Data from similar machines/ settings



Next Generation Performance Monitoring

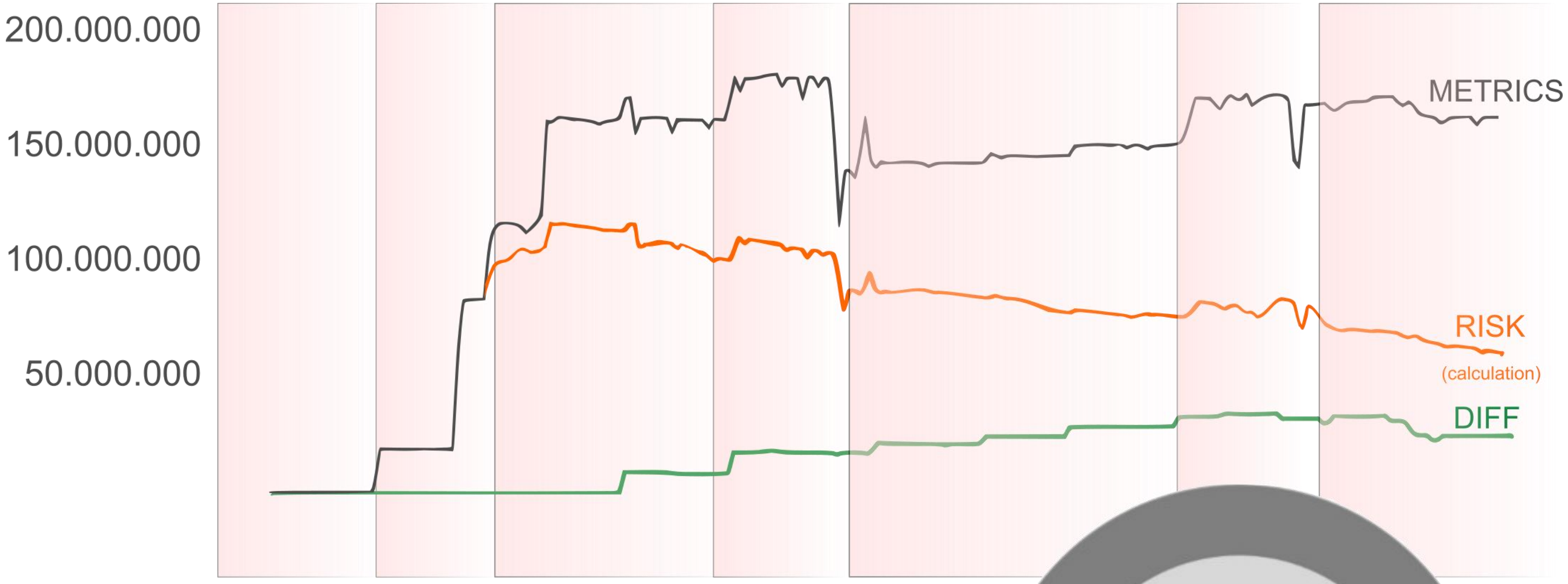
Recent Trends

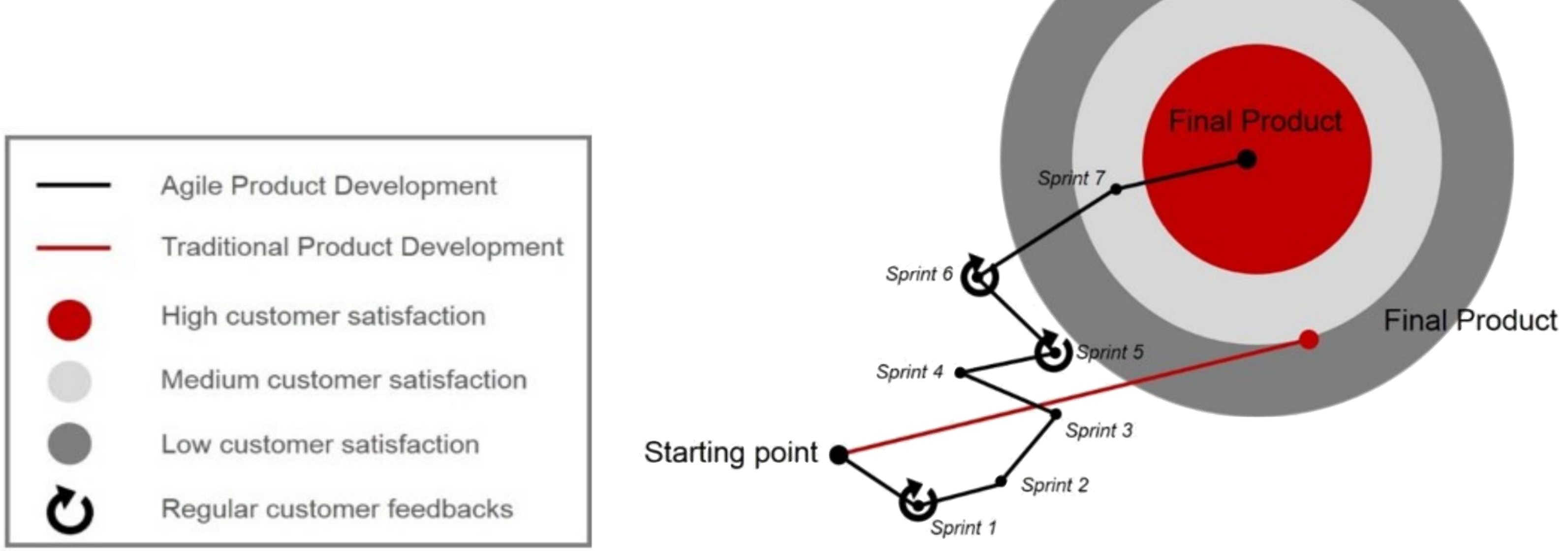
Reactivity → Proactivity

Standard Stats → Advanced Stats & Machine Learning

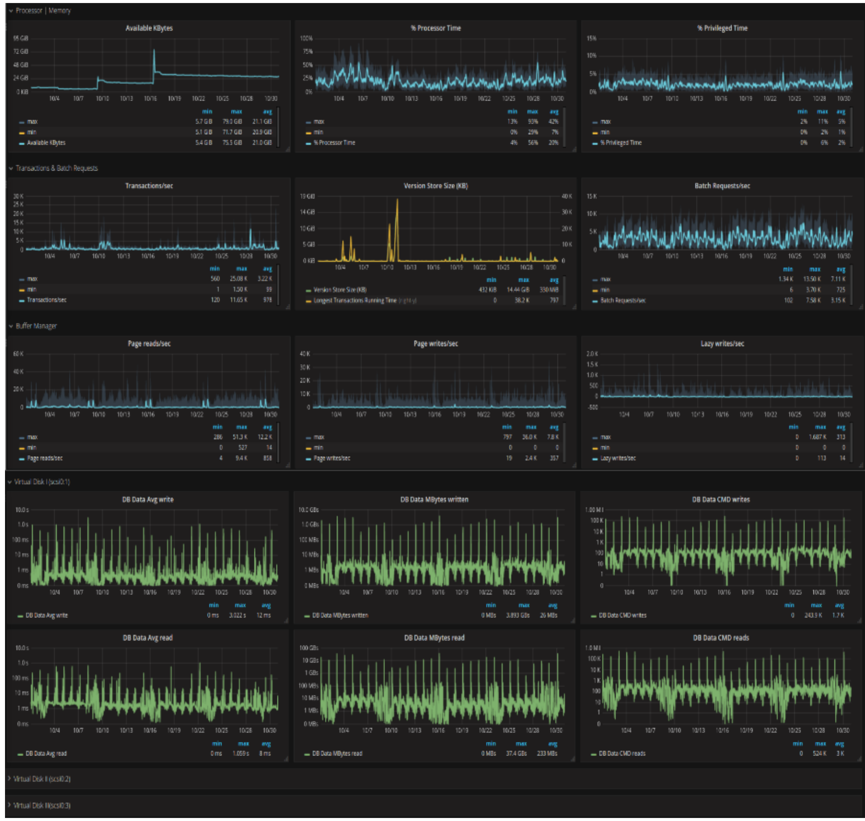
Combination of Performance Monitoring and User Experience

Agile Implementation of Solutions





Agile Product Development
Traditional Product Development
High customer satisfaction
Medium customer satisfaction
Low customer satisfaction
Regular customer feedbacks
Final Product
Sprint 7
Sprint 6
Sprint 5
Sprint 4
Sprint 3
Sprint 2
Sprint 1
Starting point
Final Product



Processor | Memory

Available KBytes

	min	max	avg
max	5.7 GiB	79.0 GiB	21.1 GiB
min	5.1 GiB	71.7 GiB	20.9 GiB
Available KBytes	5.4 GiB	75.5 GiB	21.0 GiB

% Processor Time

	min	max	avg
max	13%	93%	42%
min	0%	29%	7%
% Processor Time	4%	56%	20%

% Privileged Time

	min	max	avg
max	2%	11%	5%
min	0%	2%	1%
% Privileged Time	0%	6%	2%

Transactions & Batch Requests

Transactions/sec

	min	max	avg
max	560	25.08 K	3.22 K
min	1	1.50 K	99
Transactions/sec	120	11.65 K	978

Version Store Size (KB)

	min	max	avg
Version Store Size (KB)	432 KiB	14.44 GiB	330 MiB
Longest Transactions Running Time (right-y)	0	38.2 K	797

Batch Requests/sec

	min	max	avg
max	1.34 K	13.50 K	7.11 K
min	6	3.70 K	725
Batch Requests/sec	102	7.58 K	3.15 K

Buffer Manager

Page reads/sec

	min	max	avg
max	286	51.3 K	12.2 K
min	0	527	14
Page reads/sec	4	9.4 K	858

Page writes/sec

	min	max	avg
max	797	36.0 K	7.8 K
min	0	0	0
Page writes/sec	19	2.4 K	357

Lazy writes/sec

	min	max	avg
max	0	1.687 K	313
min	0	0	0
Lazy writes/sec	0	113	14

Virtual Disk I (scsi0:1)

DB Data Avg write

	min	max	avg
DB Data Avg write	0 ms	3.022 s	12 ms

DB Data MBytes written

	min	max	avg
DB Data MBytes written	0 MBs	3.893 GBs	26 MBs

DB Data CMD writes

	min	max	avg
DB Data CMD writes	0	243.9 K	1.7 K

DB Data Avg read

	min	max	avg
DB Data Avg read	0 ms	1.059 s	8 ms

DB Data MBytes read

	min	max	avg
DB Data MBytes read	0 MBs	37.4 GBs	233 MBs

DB Data CMD reads

	min	max	avg
DB Data CMD reads	0	524 K	3 K

Virtual Disk II (scsi0:2)

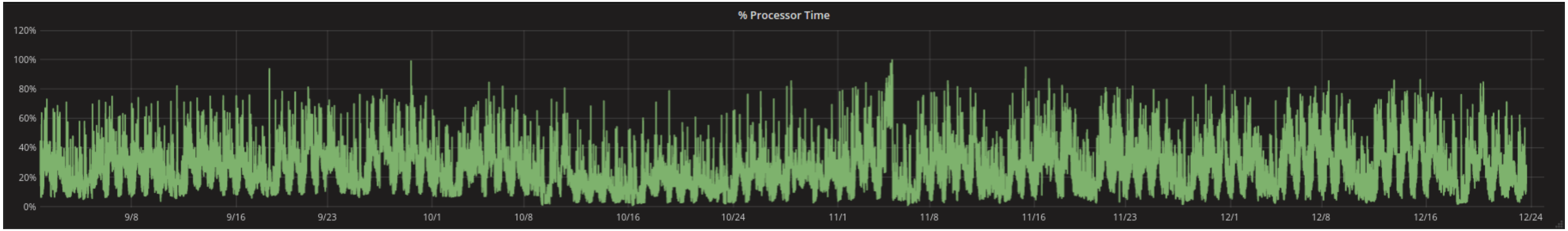
Virtual Disk III(scsi0:3)

Customer specific solutions with agile implementation

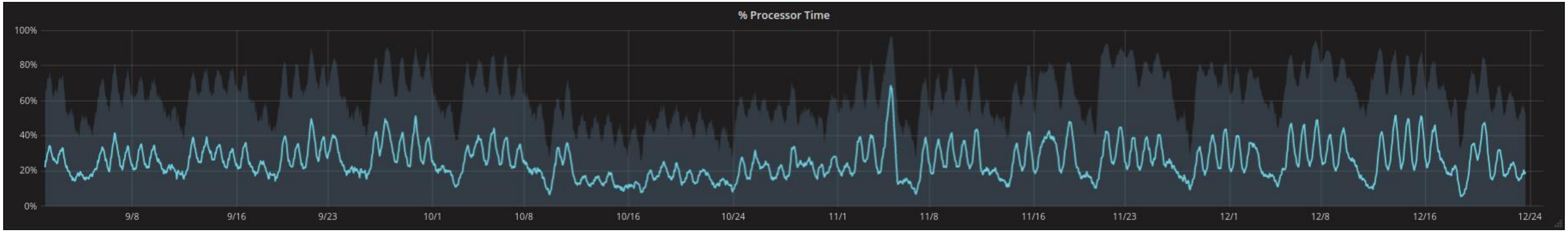
REACTIVITY → PROACTIVITY

Visualization: Trend Detection

VORHER



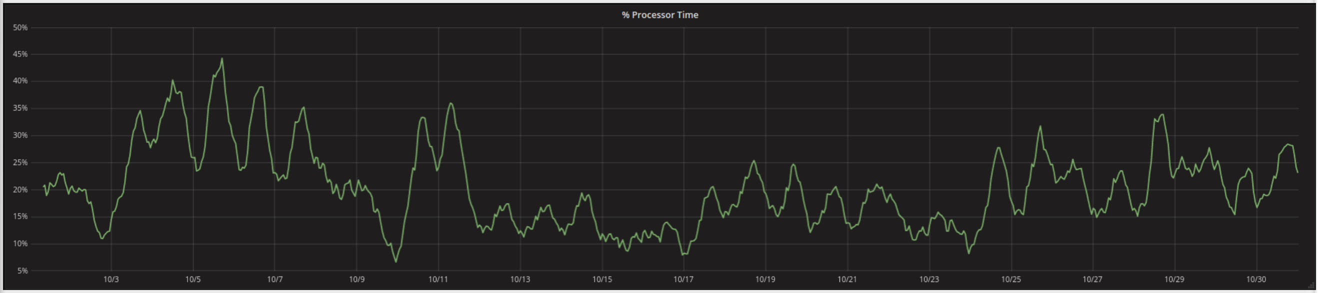
NACHHER



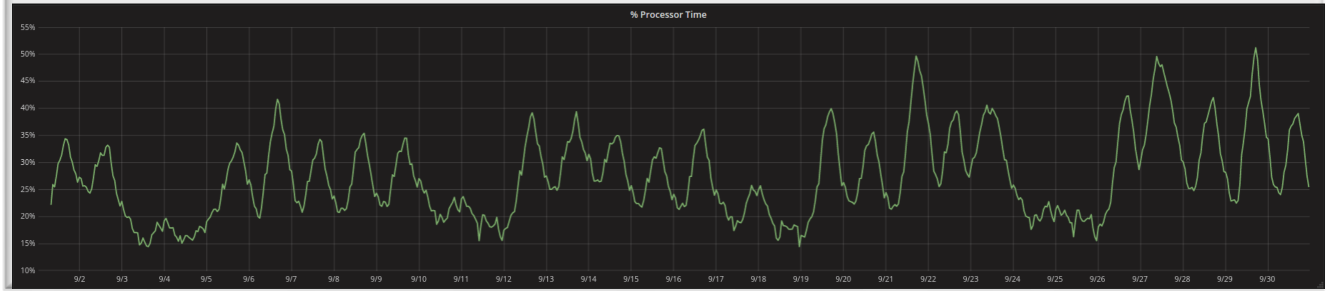
- Areas not to many points
- Smoothed signal

Historic Data

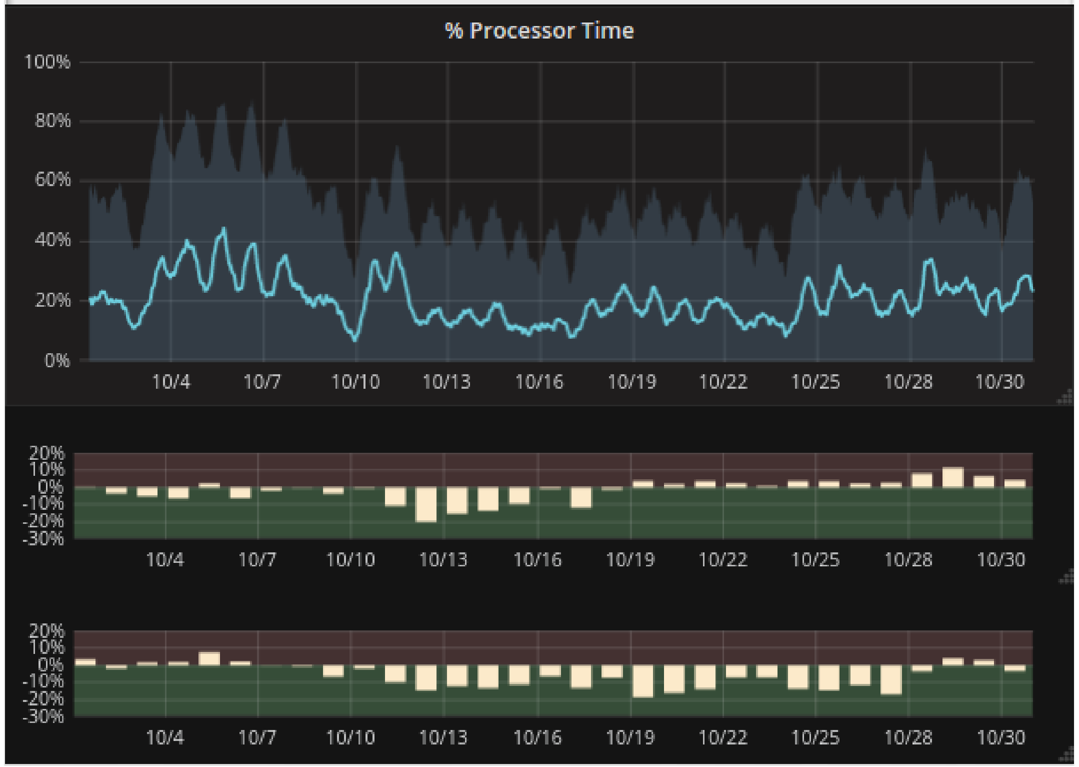
VORHER



- Comparison time consuming
- Quantification complicated



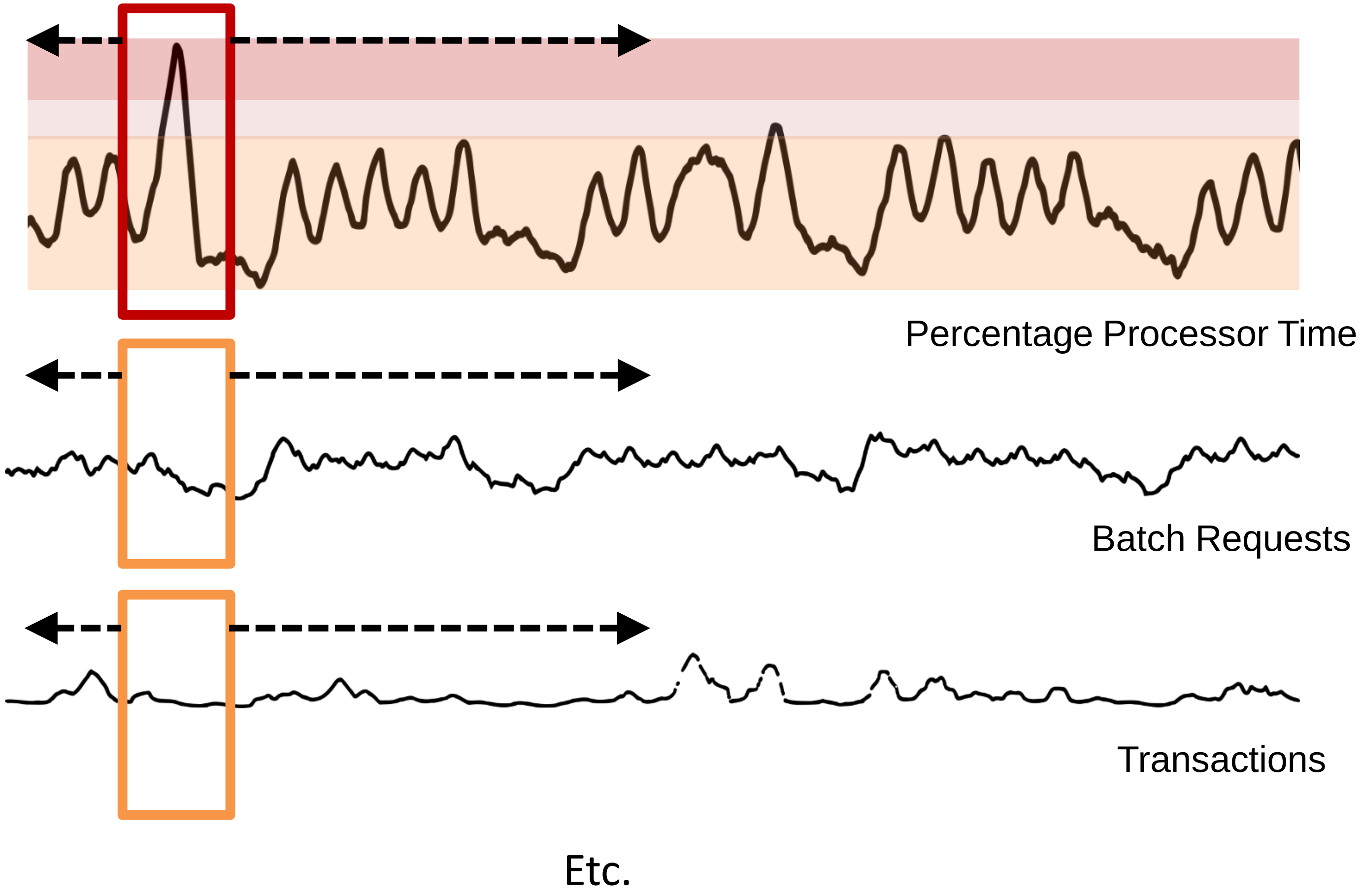
NACHHER



- Historic data at hand
- Visualization of differences
  => Easy trend detection

STANDARD STATS → ADVANCED STATS & ML

Univariate Data Analysis

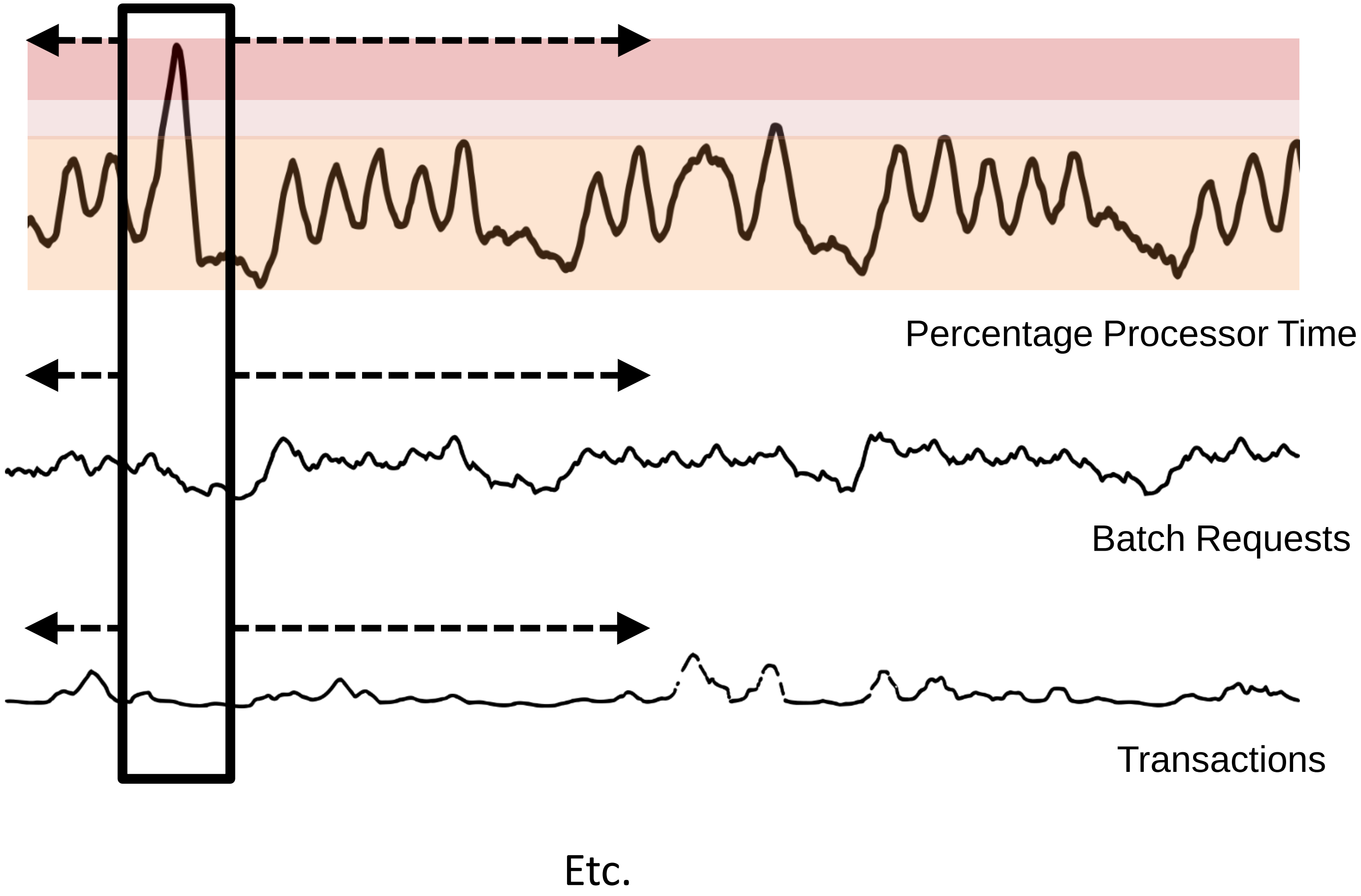


- Every time series is analyzed on **separately**
- Thresholds are calculated on via **baselining**
- Alarms from separate time series are combined into a **global alarm**
- Relationships between time series are **ignored**
- Shape of time series is **ignored**

Motivations

- Separate Data Sources
- Different Precision
- Evolution of networks (complexity)
- Common practice was enough

Multi-variate Data Analysis

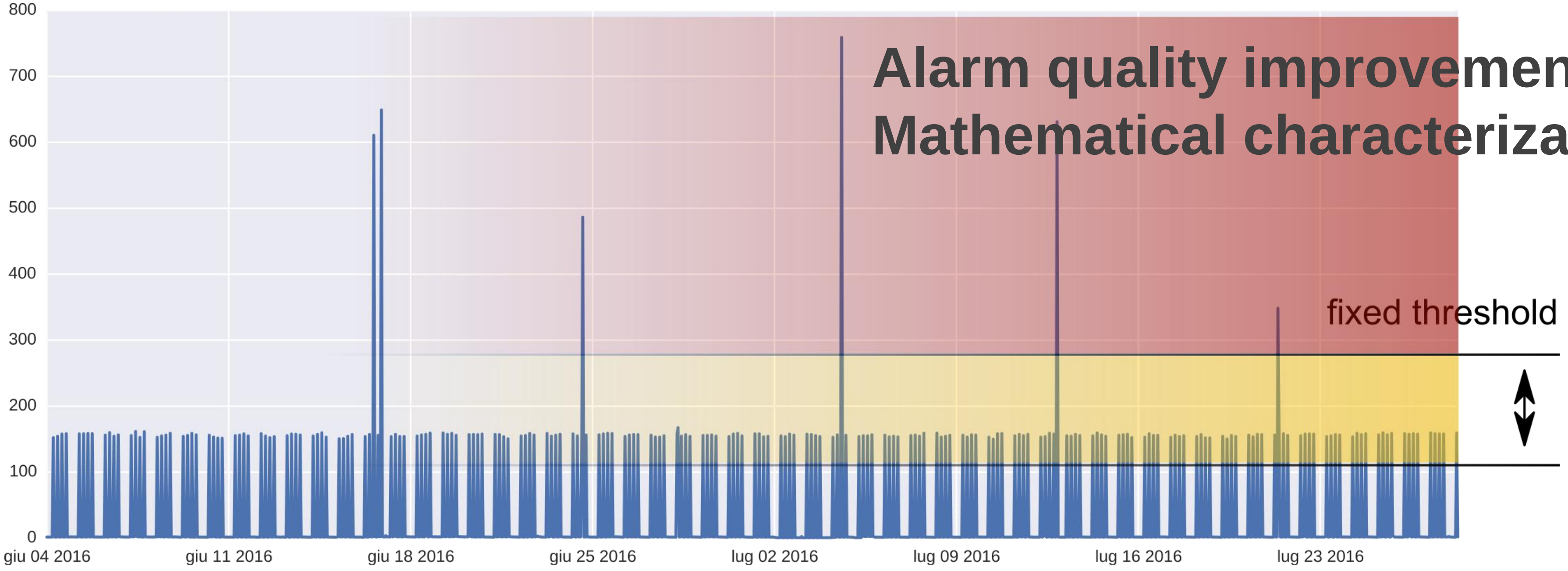


- All time series are analyzed on **together**
- Thresholds are calculated dynamically via **baselining and anomaly detection**
- **Risk estimation** in addition to **global alarm and specific alarms**
- Relationships between time series are used to create more reliable alarms and risks
- Shape of time series is **considered**

Motivations

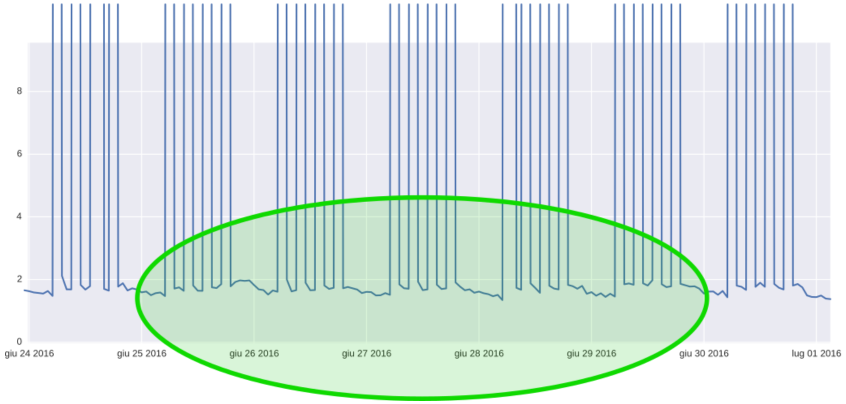
- Common Data Source
- Grafana & InfluxDB
- Today we need more than common practice
- **Proactivity**

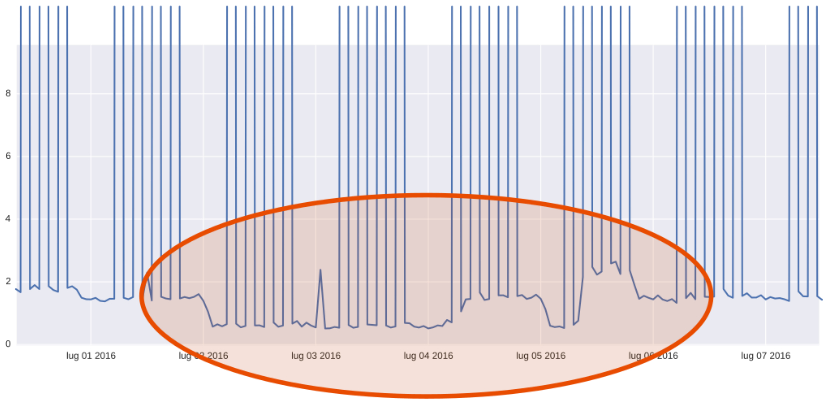
Anomaly vs. Threshold



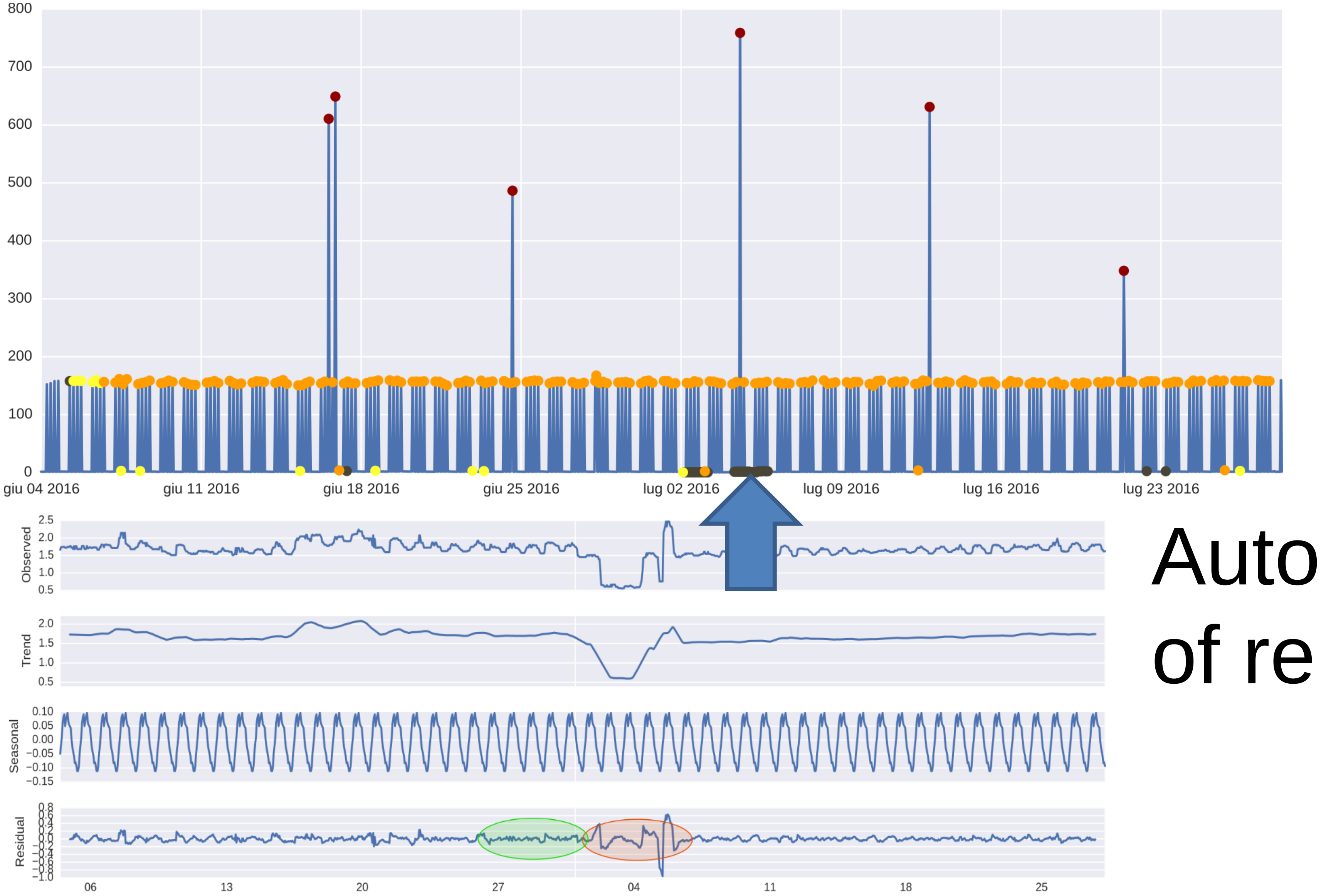
Alarm quality improvement

Mathematical characterization of standard traffic





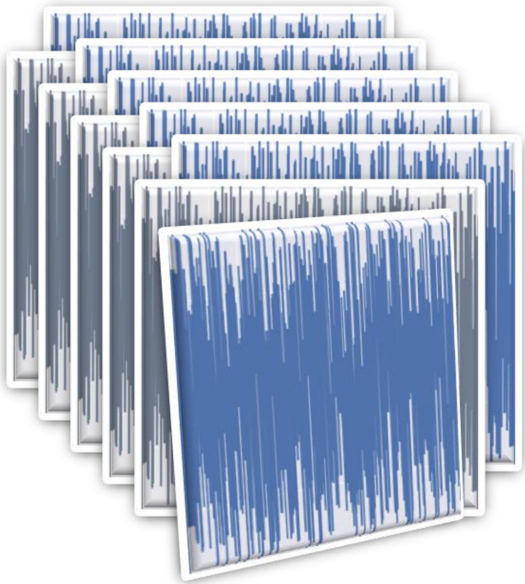
Anomaly vs. Threshold



Automatic detection of relevant changes

Risk: Anomaly Detection via Multivariate ML Analysis

Metrics



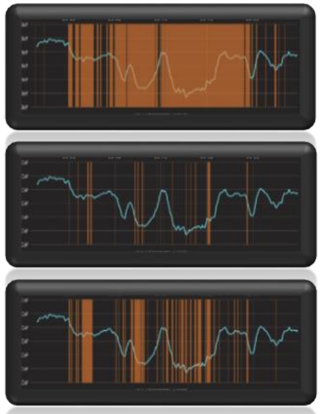
MODEL
STANDARD
BEHAVIOUR

- historical data of same metric
- historical data of similar metric
- historical data of similar machine

WHAT DO WE EXPECT?

- The farer away from expectation the higher the RISK
- RISK: different and rare

HOW FAR ARE WE FROM OUR EXPECTATION?



RISK
SCORE

Risk: Culprit Detection with Risk

IOs

HIGH RISK PERIODS

- historical data of same metric
- historical data of similar metric
- historical data of similar machine
- historical data of neighbours

AUTOMATED ANALYSIS

- Which (set of) machine(s) is most probably causing the high risk
- Proactive analysis to prevent congestion

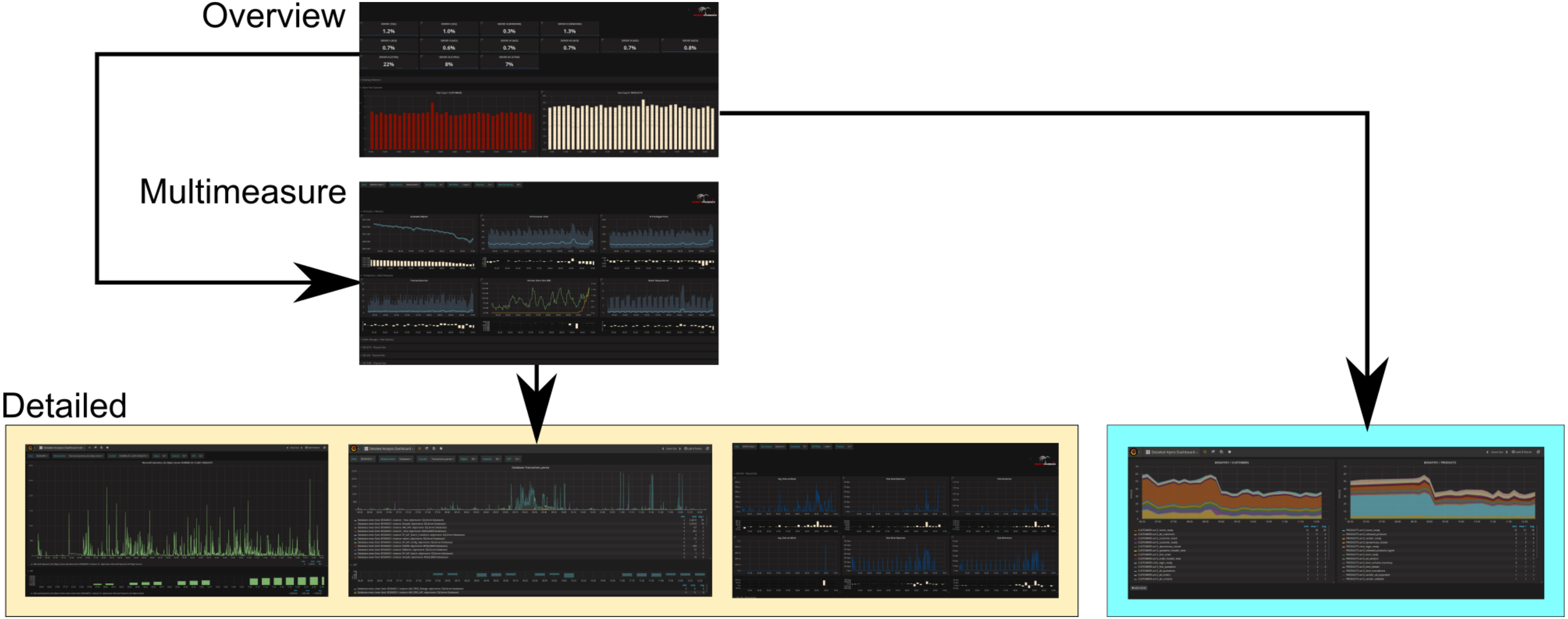
Proactive search for potential future culprits

Faster Troubleshooting

- Check machines with high risk first, there might be no need to control the others

COMBINATION OF PERFORMANCE MONITORING AND USER EXPERIENCE

3 Levels of Dashboards

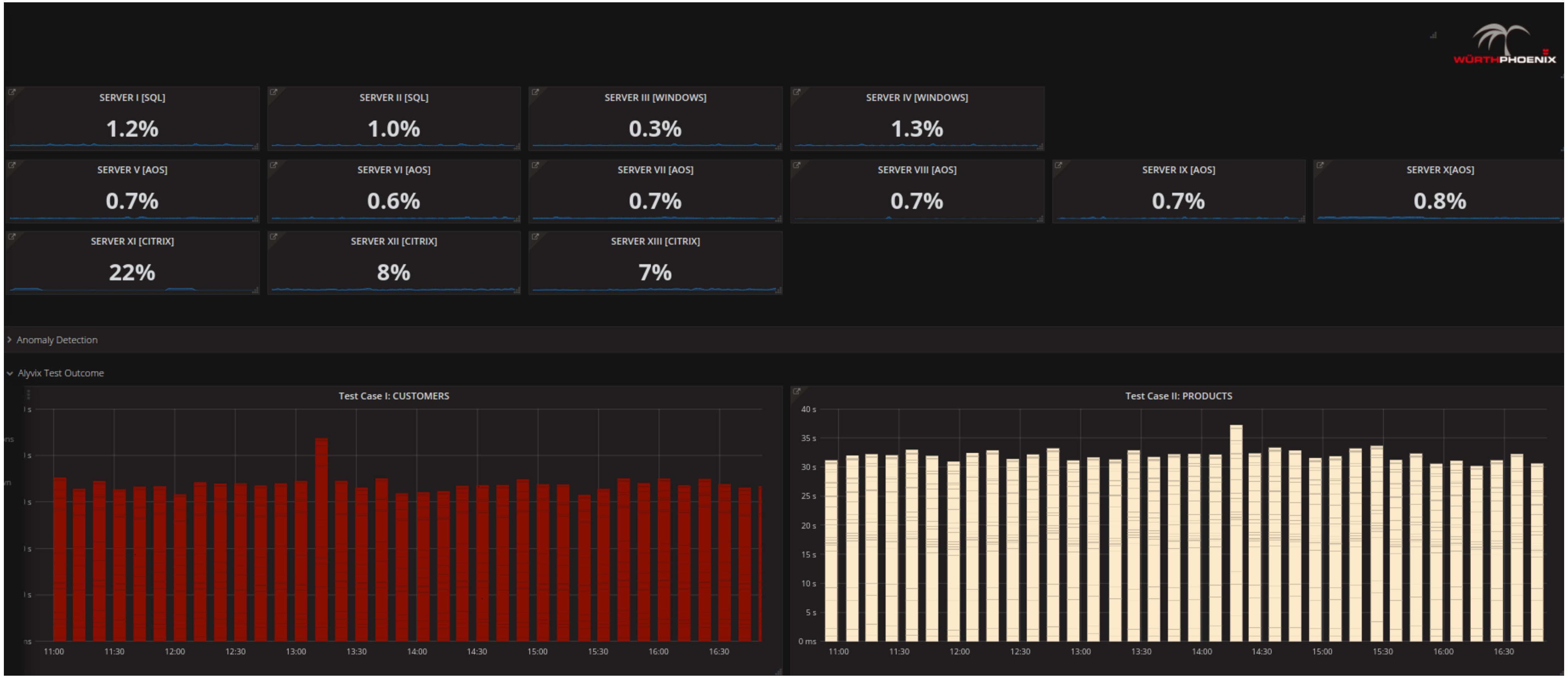


Overview

Multimeasure

Detailed

Level 1: Overview Dashboard



SERVER I [SQL] 1.2%

SERVER II [SQL] 1.0%

SERVER III [WINDOWS] 0.3%

SERVER IV [WINDOWS] 1.3%

SERVER V [AOS] 0.7%

SERVER VI [AOS] 0.6%

SERVER VII [AOS] 0.7%

SERVER VIII [AOS] 0.7%

SERVER IX [AOS] 0.7%

SERVER X[AOS] 0.8%

SERVER XI [CITRIX] 22%

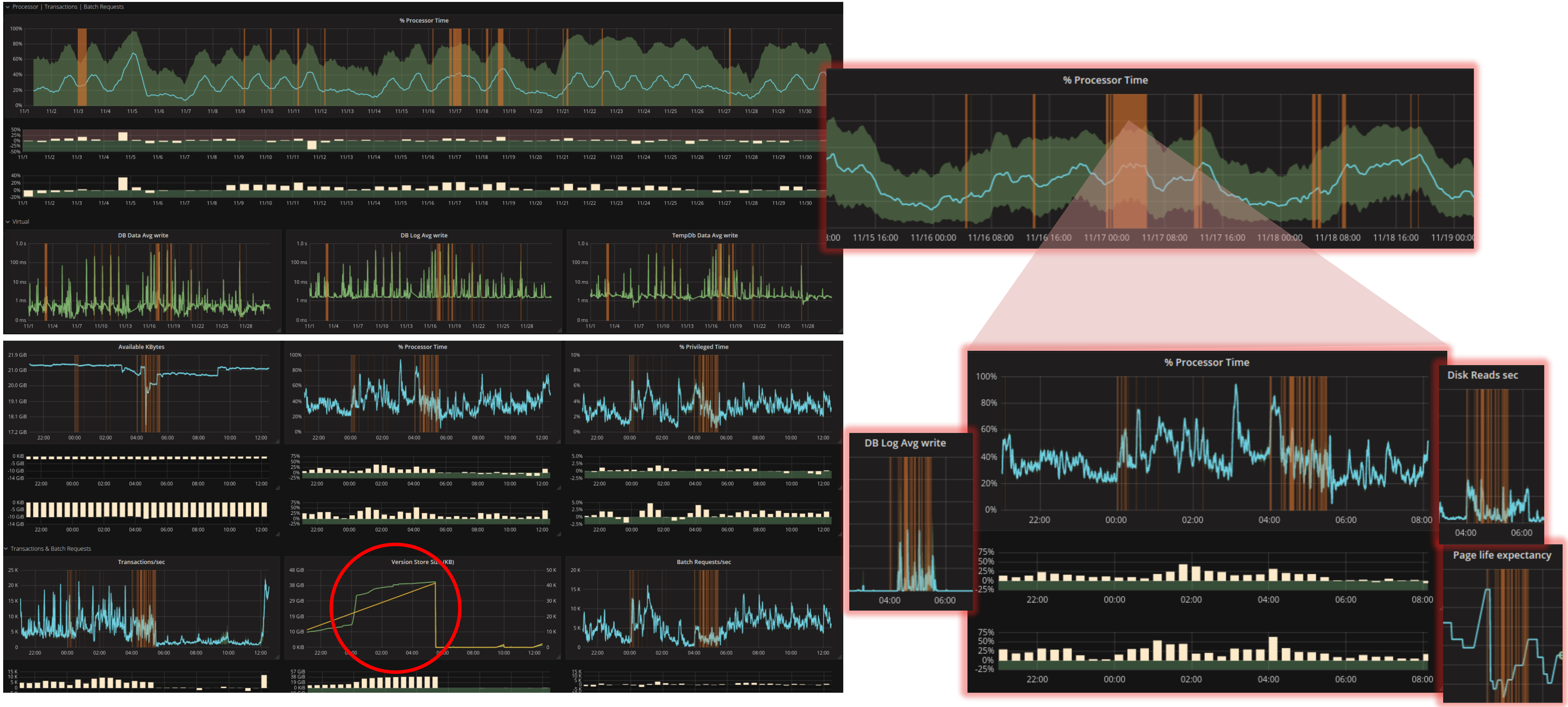
SERVER XII [CITRIX] 8%

SERVER XIII [CITRIX] 7%

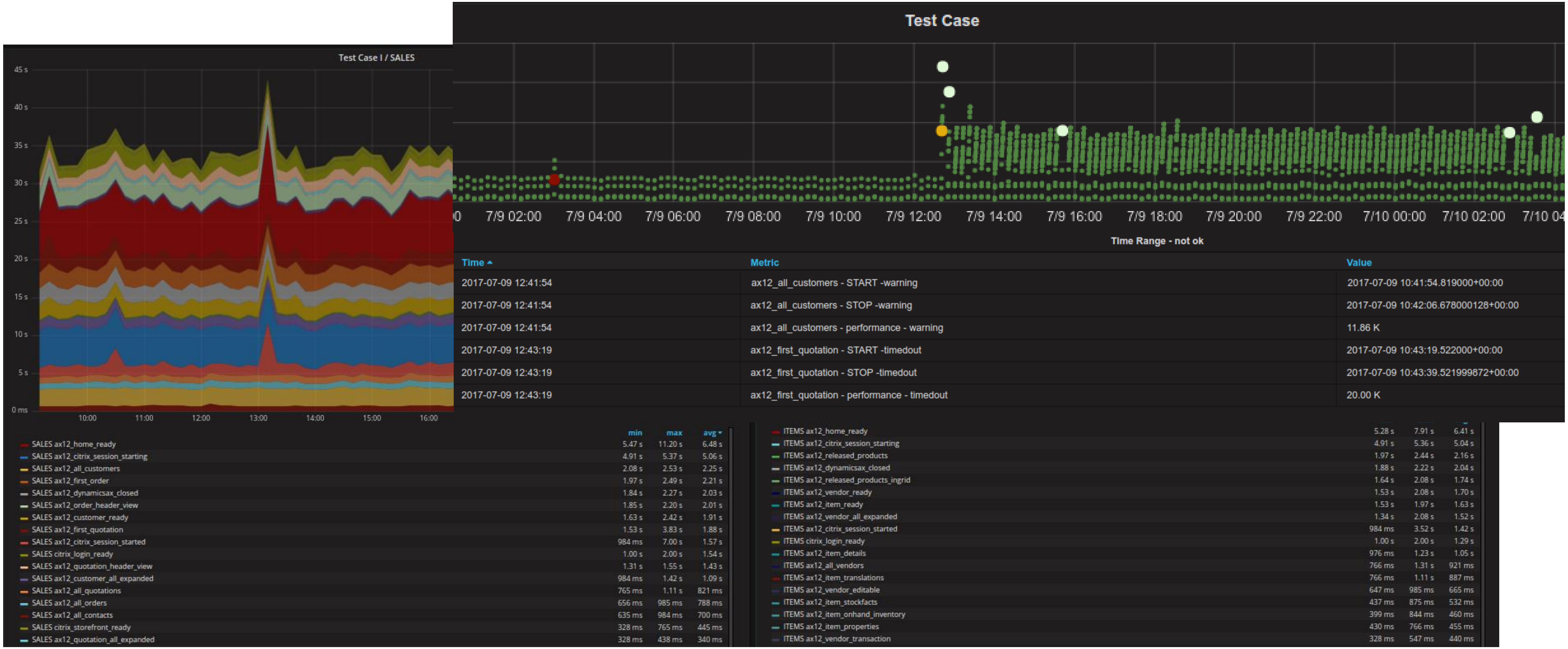
Server Overview

User Experience Overview

Level 2: Multimeasure - Troubleshooting



Detailed Dashboard (Alyvix)



Time ▲	Metric	Value
2017-07-09 12:41:54	ax12_all_customers - START -warning	2017-07-09 10:41:54.819000+00:00
2017-07-09 12:41:54	ax12_all_customers - STOP -warning	2017-07-09 10:42:06.678000128+00:00
2017-07-09 12:41:54	ax12_all_customers - performance - warning	11.86 K
2017-07-09 12:43:19	ax12_first_quotation - START -timedout	2017-07-09 10:43:19.522000+00:00
2017-07-09 12:43:19	ax12_first_quotation - STOP -timedout	2017-07-09 10:43:39.521999872+00:00
2017-07-09 12:43:19	ax12_first_quotation - performance - timedout	20.00 K

	min	max	avg ▾
SALES ax12_home_ready	5.47 s	11.20 s	6.48 s
SALES ax12_citrix_session_starting	4.91 s	5.37 s	5.06 s
SALES ax12_all_customers	2.08 s	2.53 s	2.25 s
SALES ax12_first_order	1.97 s	2.49 s	2.21 s
SALES ax12_dynamicsax_closed	1.84 s	2.27 s	2.03 s
SALES ax12_order_header_view	1.85 s	2.20 s	2.01 s
SALES ax12_customer_ready	1.63 s	2.42 s	1.91 s
SALES ax12_first_quotation	1.53 s	3.83 s	1.88 s
SALES ax12_citrix_session_started	984 ms	7.00 s	1.57 s
SALES citrix_login_ready	1.00 s	2.00 s	1.54 s
SALES ax12_quotation_header_view	1.31 s	1.55 s	1.43 s
SALES ax12_customer_all_expanded	984 ms	1.42 s	1.09 s
SALES ax12_all_quotations	765 ms	1.11 s	821 ms
SALES ax12_all_orders	656 ms	985 ms	788 ms
SALES ax12_all_contacts	635 ms	984 ms	700 ms
SALES citrix_storefront_ready	328 ms	765 ms	445 ms
SALES ax12_quotation_all_expanded	328 ms	438 ms	340 ms

ITEMS ax12_home_ready	5.28 s	7.91 s	6.41 s
ITEMS ax12_citrix_session_starting	4.91 s	5.36 s	5.04 s
ITEMS ax12_released_products	1.97 s	2.44 s	2.16 s
ITEMS ax12_dynamicsax_closed	1.88 s	2.22 s	2.04 s
ITEMS ax12_released_products_ingrid	1.64 s	2.08 s	1.74 s
ITEMS ax12_vendor_ready	1.53 s	2.08 s	1.70 s
ITEMS ax12_item_ready	1.53 s	1.97 s	1.63 s
ITEMS ax12_vendor_all_expanded	1.34 s	2.08 s	1.52 s
ITEMS ax12_citrix_session_started	984 ms	3.52 s	1.42 s
ITEMS citrix_login_ready	1.00 s	2.00 s	1.29 s
ITEMS ax12_item_details	976 ms	1.23 s	1.05 s
ITEMS ax12_all_vendors	766 ms	1.31 s	921 ms
ITEMS ax12_item_translations	766 ms	1.11 s	887 ms
ITEMS ax12_vendor_editable	647 ms	985 ms	665 ms
ITEMS ax12_item_stockfacts	437 ms	875 ms	532 ms
ITEMS ax12_item_onhand_inventory	399 ms	844 ms	460 ms
ITEMS ax12_item_properties	430 ms	766 ms	455 ms
ITEMS ax12_vendor_transaction	328 ms	547 ms	440 ms

GRAZIE!