



Webinar

# Advanced problem detection

all our microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

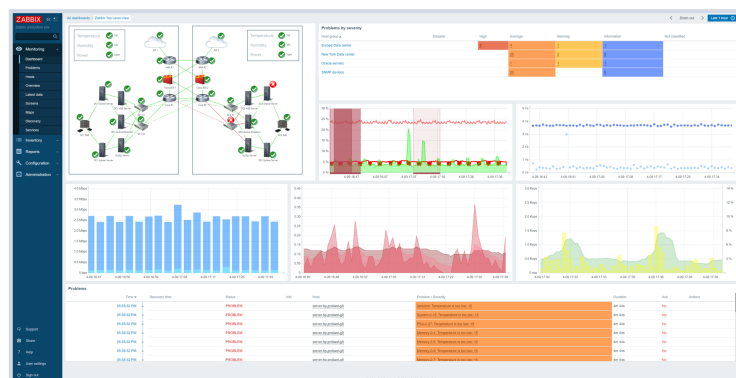
1

# Zabbix data flow



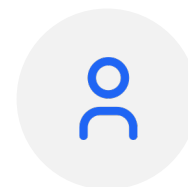
## ADVANCED PROBLEM DETECTION

# Zabbix data flow



Visualization

Notifications



DATABASE

ZABBIX SERVER

History

Analysis



Data collection

## ADVANCED PROBLEM DETECTION

# How often to execute checks?

### Every N seconds

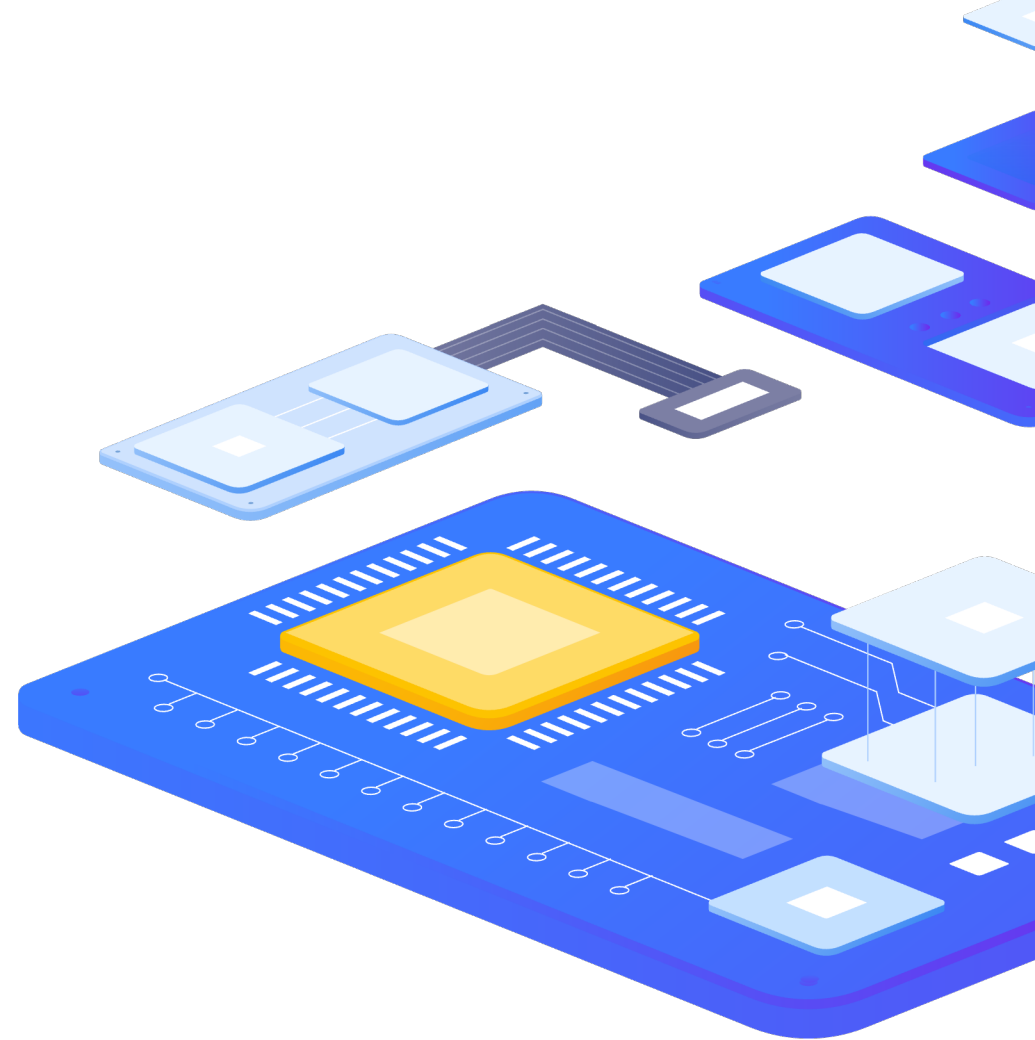
- › Zabbix will evenly distribute checks

### Different frequency in different time periods

- › Every X seconds in working time
- › Every Y second in weekend

### At a specific time (Zabbix 3.0)

- › Ready for business checks
- › Every hour starting from 9:00 at working hours (9:00, 10:00,..., 18:00)



# 2

## Triggers



## ADVANCED PROBLEM DETECTION

# Trigger – problem definition

### Example

› `last(/server/system.cpu.load) > 5`

### Operators

› `- + / * < > = <> >= <= not or and`

### Functions

› `min max avg last count date time diff regexp` and much more!

### Analyze everything: any metric and any host

› `last(/node1/system.cpu.load) > 5 and last(/node2/system.cpu.load) > 5 and last(/nodes/tps) < 5000`

# Trigger Functions

Function group	Functions
Aggregate functions	avg, bucket_percentile, count, histogram_quantile, item_count, kurtosis, mad, max, min, skewness, stddevpop, stddevsamp, sum, sumofsquares, varpop, varsamp
Bitwise functions	bitand, bitlshift, bitnot, bitor, bitrshift, bitxor
Date and time functions	date, dayofmonth, dayofweek, now, time
History functions	baselinedev, baselinewma, change, changecount, count, countunique, find, first, fuzzytime, last, logeventid, logseverity, logsource, monodec, monoinc, nodata, percentile, rate, trendavg, trendcount, trendmax, trendmin, trendstl, trendsum
Mathematical functions	abs, acos, asin, atan, atan2, avg, cbrt, ceil, cos, cosh, cot, degrees, e, exp, expm1, floor, log, log10, max, min, mod, pi, power, radians, rand, round, signum, sin, sinh, sqrt, sum, tan, truncate
Operator functions	between, in
Prediction functions	forecast, timeleft
String functions	ascii, bitlength, bytelength, char, concat, insert, left, length, ltrim, mid, repeat, replace, right, rtrim, trim

# Foreach Functions - tip

- › avg\_foreach
- › bucket\_rate\_foreach
- › count\_foreach
- › exists\_foreach
- › last\_foreach
- › max\_foreach
- › min\_foreach
- › sum\_foreach

## Calculated Items on:

### Host level

- › `sum(last_foreach(/host/net.if.in[*]))`

### Hostgroup level

- › `avg_foreach(/*/mysql.qps?[group="MySQL Servers"],5m)`



## ADVANCED PROBLEM DETECTION

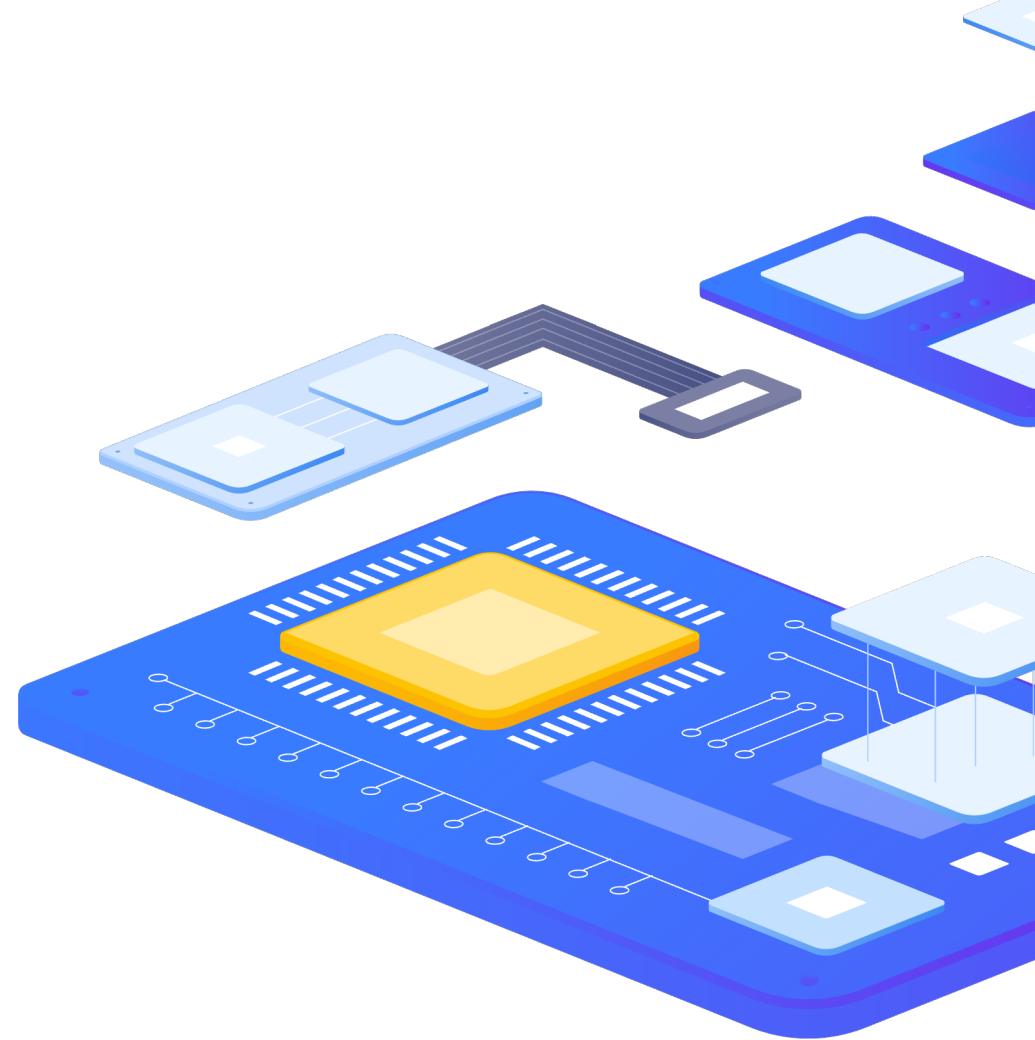
# Junior level

### Performance

- › `last(/server/system.cpu.load) > 5`

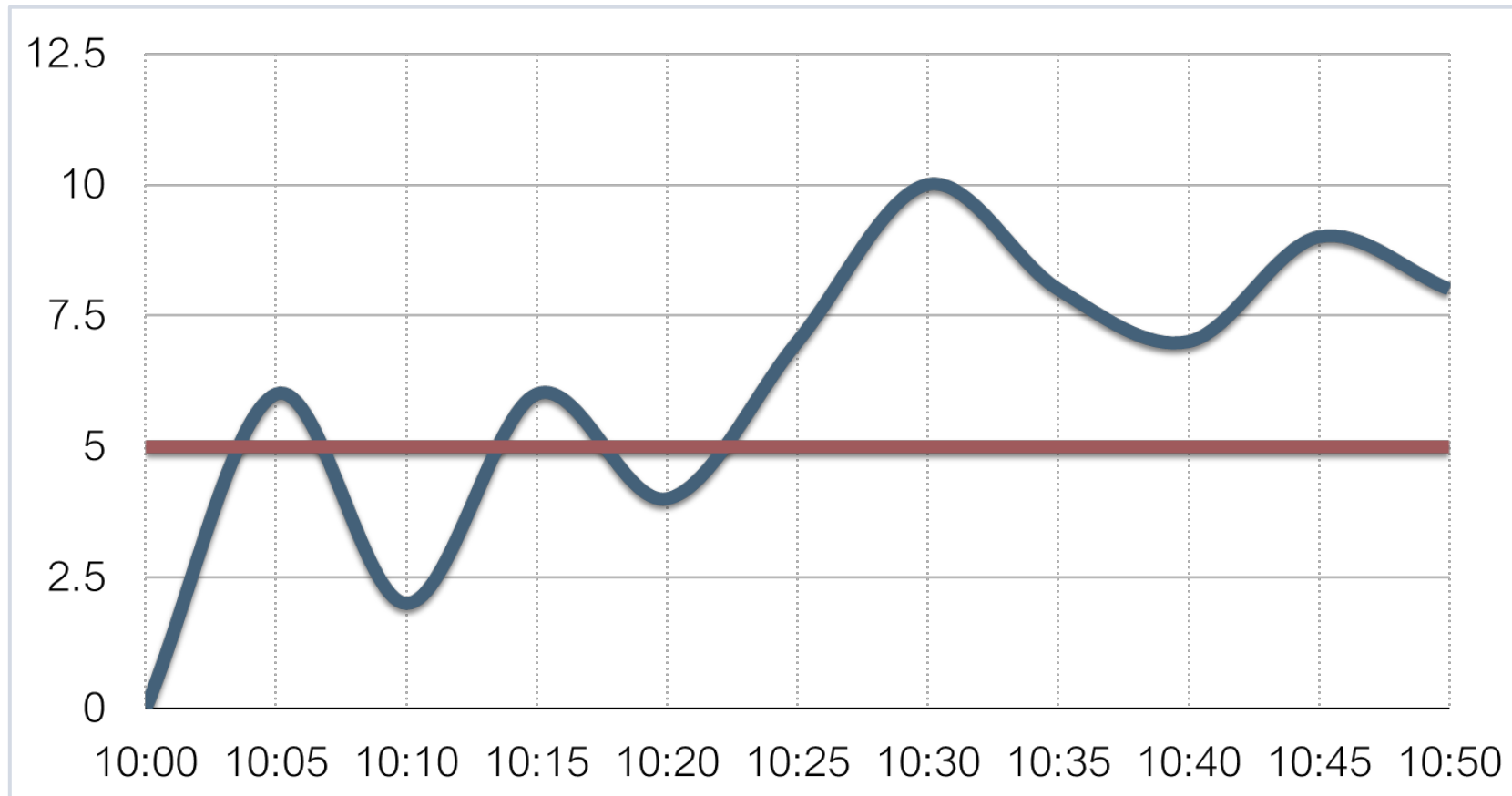
### Availability

- › `last(/server/net.tcp.service[http]) = 0`



## ADVANCED PROBLEM DETECTION

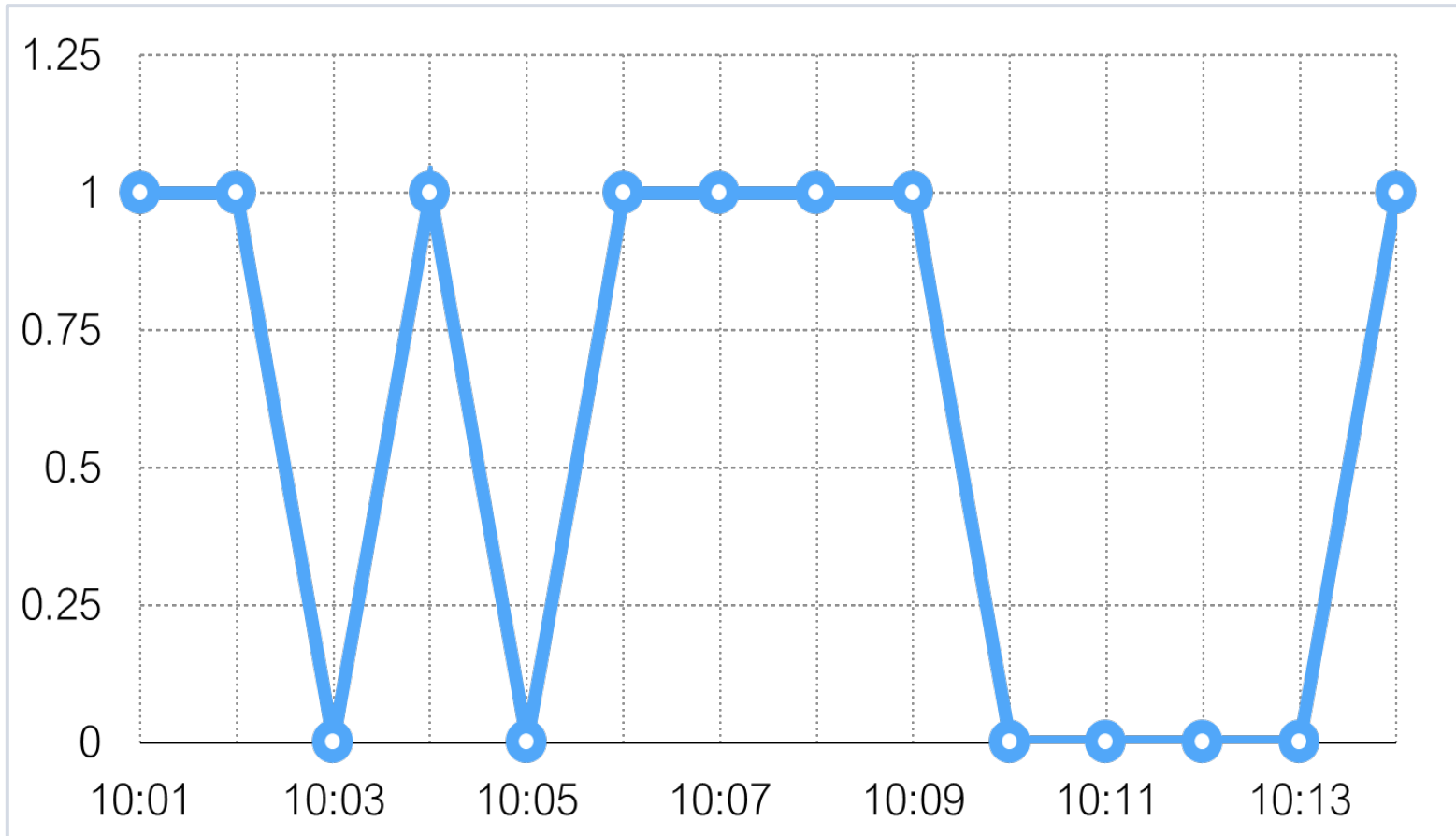
# False positives



`last(/server/system.cpu.load) > 5`

## ADVANCED PROBLEM DETECTION

# Too sensitive



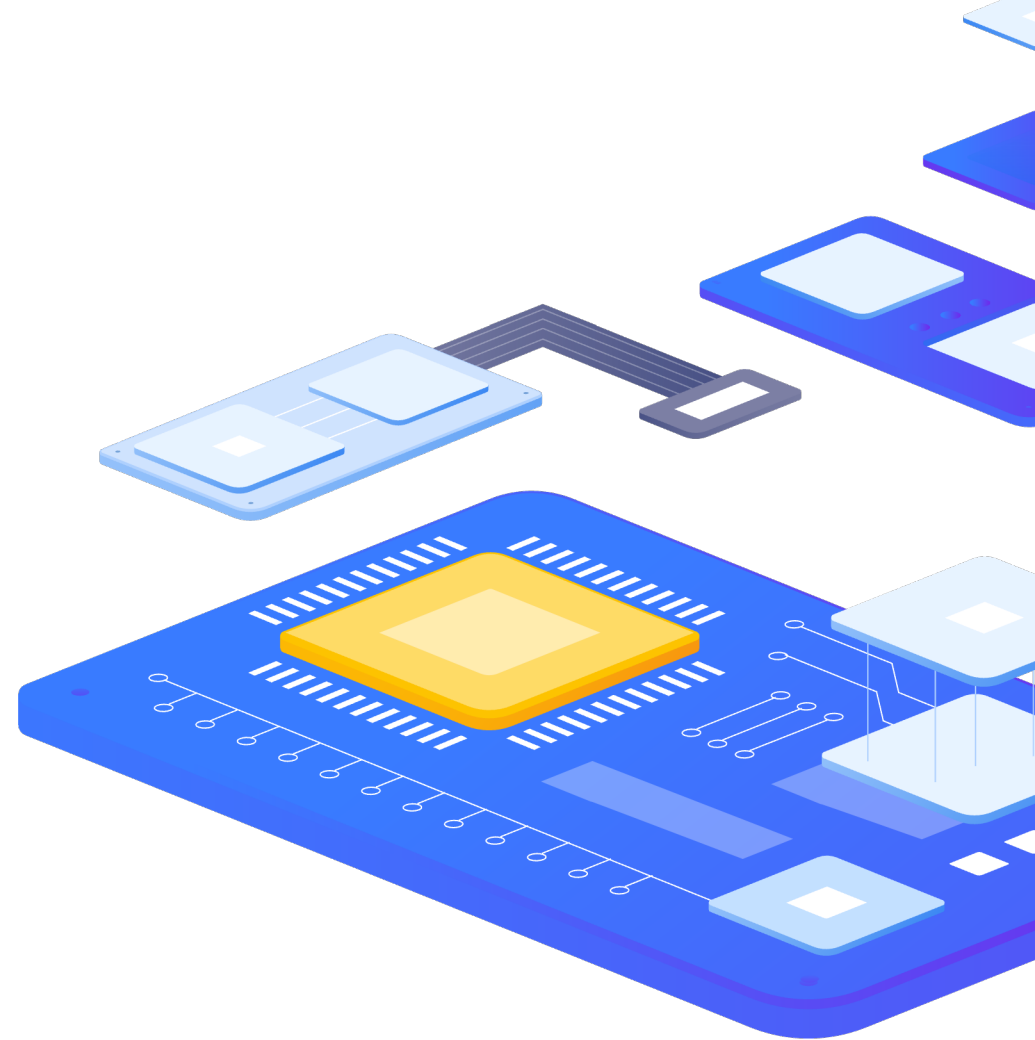
`last(/server/net.tcp.service[http]) = 0`

Advanced problem detection

# Junior level

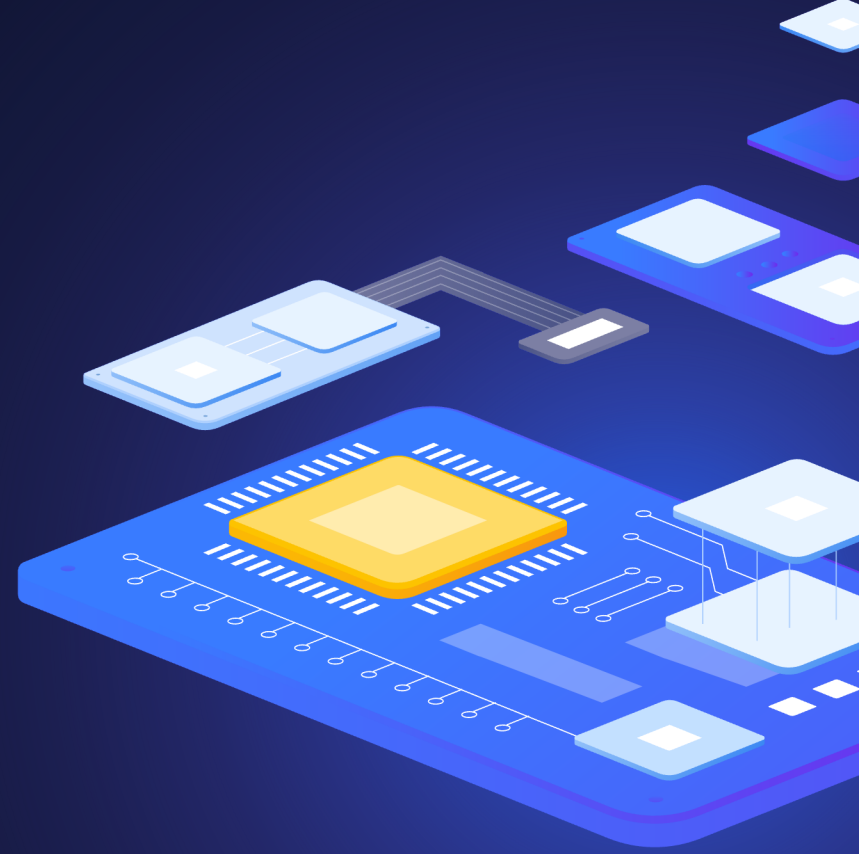
**Too sensitive leads to**

- ▶ False positives



3

False positives



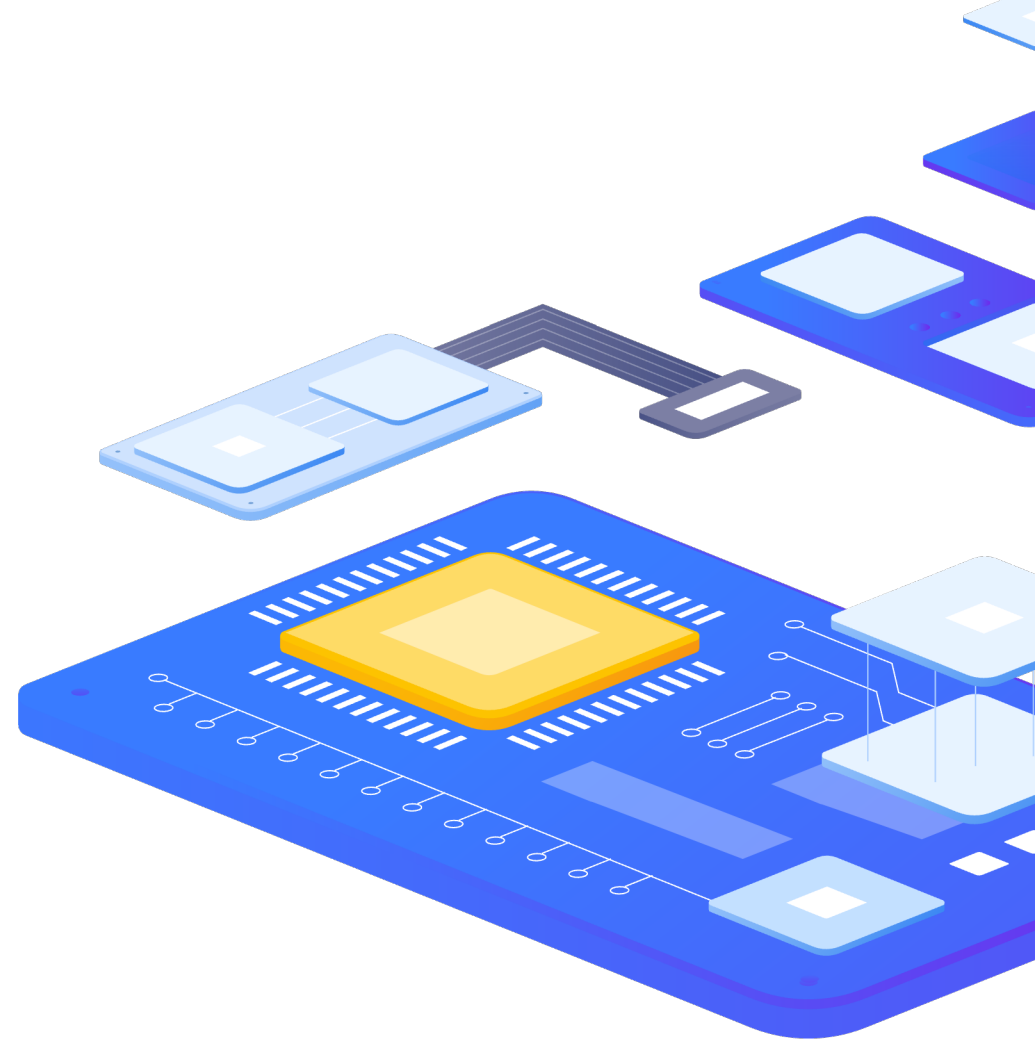
## ADVANCED PROBLEM DETECTION

# How to avoid false positives?

Be careful and define problems wisely!

What does it really mean?

- › system is overloaded
- › application does not work
- › service is not available



## ADVANCED PROBLEM DETECTION

# Examples

### Problem:

- › CPU load > 5

### No problem:

- › CPU load = 4.99 → Resolved?

### Problem:

- › free disk space < 10%

### No problem:

- › free disk space = 10.001% → Resolved?

### Problem:

- › SSH check failed

### No problem:

SSH is up → Resolved?

## ADVANCED PROBLEM DETECTION

# Analyze history

### Performance

- ›  $\min(/server/system.cpu.load, 10m) > 5$

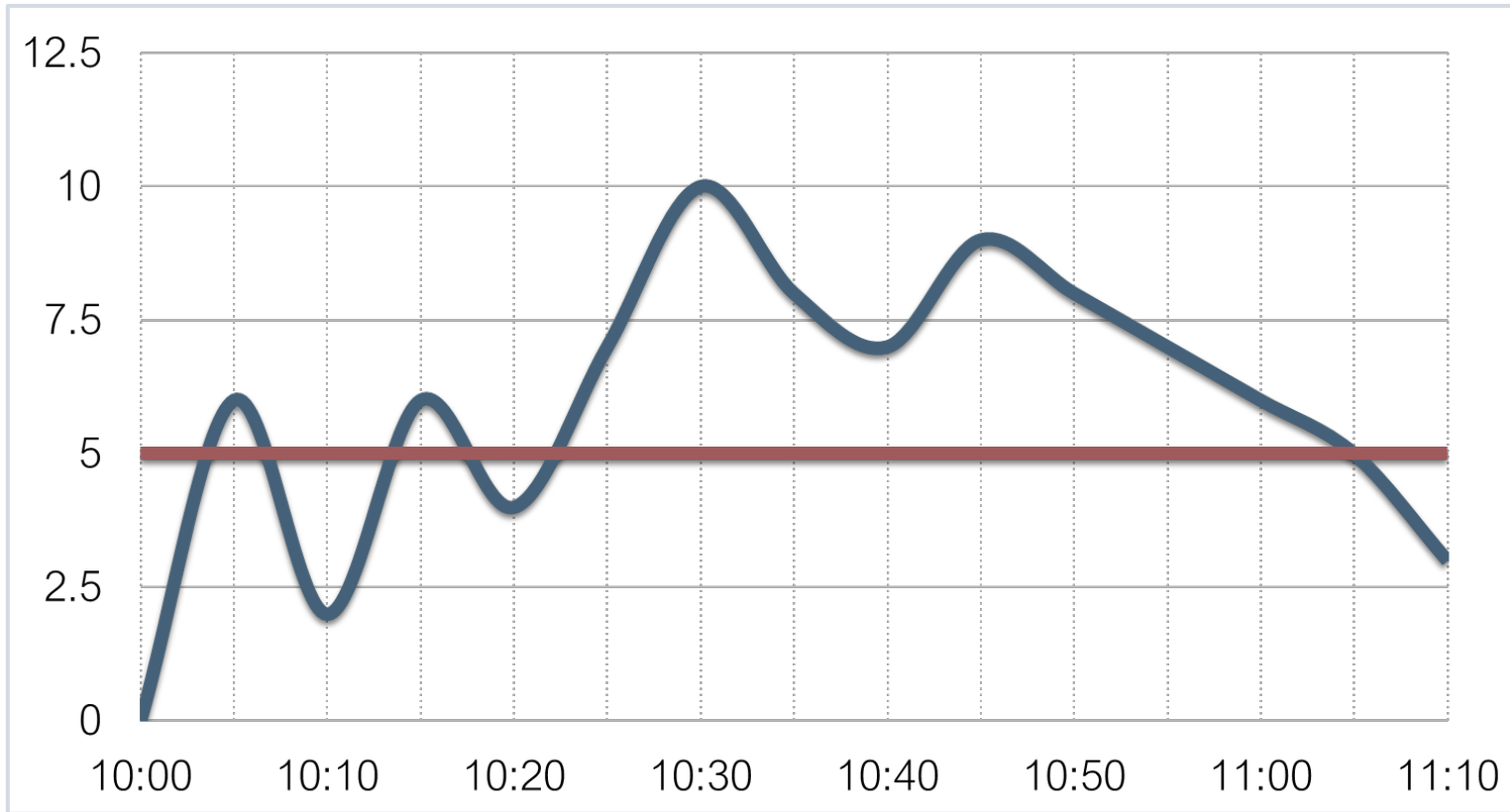
### Availability

- ›  $\max(/server/net.tcp.service[http], 5m) = 0$
- ›  $\max(/server/net.tcp.service[http], \#3) = 0$



## ADVANCED PROBLEM DETECTION

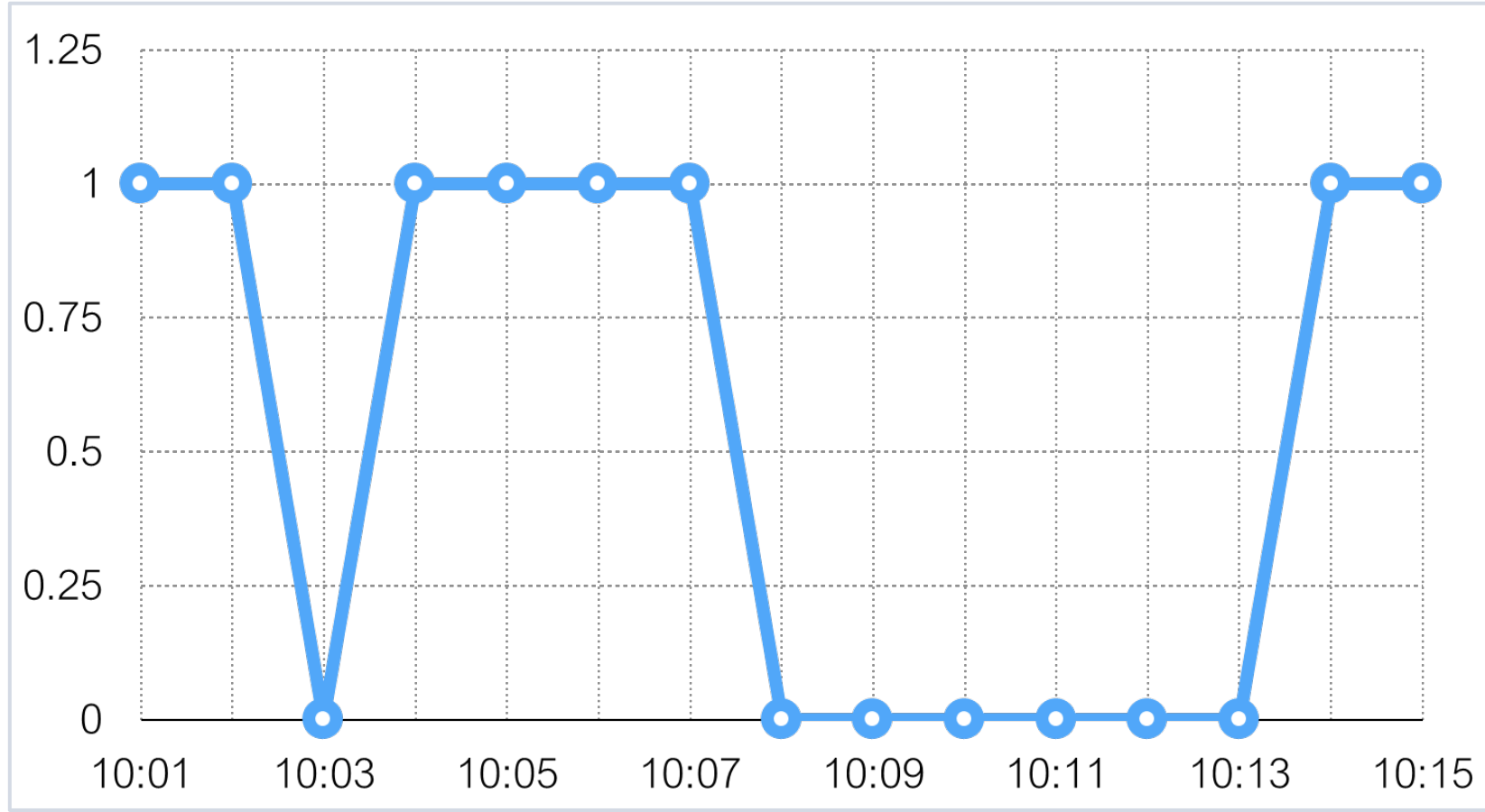
# Analyze history



`min(/server/system.cpu.load,10m) > 5`

## ADVANCED PROBLEM DETECTION

# Analyze history



`max(/server/net.tcp.service[http],#3) = 0`

## ADVANCED PROBLEM DETECTION

# Different conditions for problem and recovery

### Before

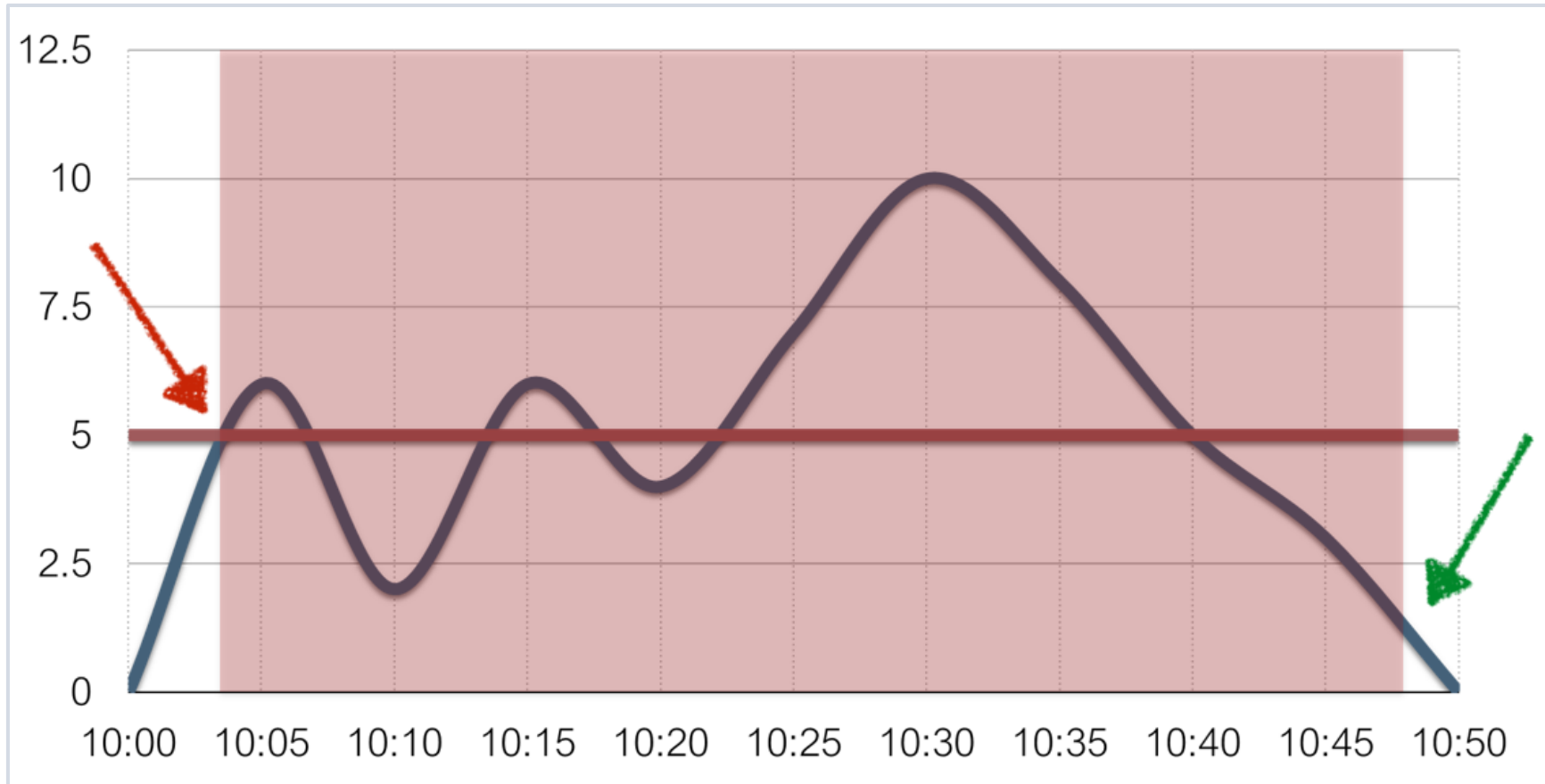
- › `last(/server/system.cpu.load) > 5`

### Now

- › Problem definition: `last(/server/system.cpu.load)>5`
- › Recovery expression: `last(/server/system.cpu.load)}<=1`

## ADVANCED PROBLEM DETECTION

# Different conditions for problem and recovery



Problem definition: `last(/server/system.cpu.load)>5` ...Recovery expression: `last(/server/system.cpu.load)}<=1`

## ADVANCED PROBLEM DETECTION

# Examples

### System is overloaded

Problem definition:

- ▶  $\min(/server/system.cpu.load, 5m) > 3$

Recovery expression:

- ▶  $\max(/server/system.cpu.load, 2m) \leq 1$

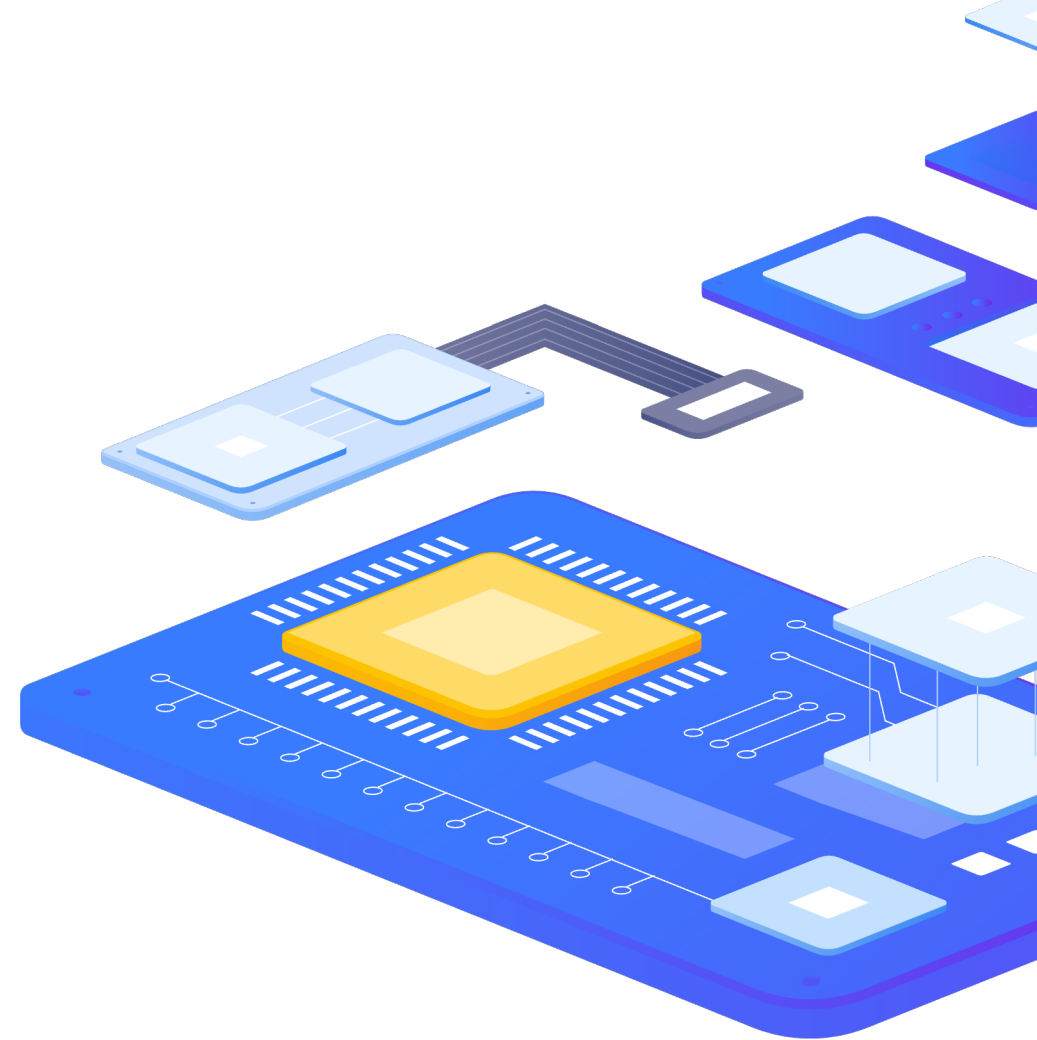
### No free disk space /

Problem definition:

- ▶  $\text{last}(/server/vfs.fs.size[/, pfree]) < 10$

Recovery expression:

- ▶  $\min(/server/vfs.fs.size[/, pfree], 15m) > 30$



## ADVANCED PROBLEM DETECTION

# Examples

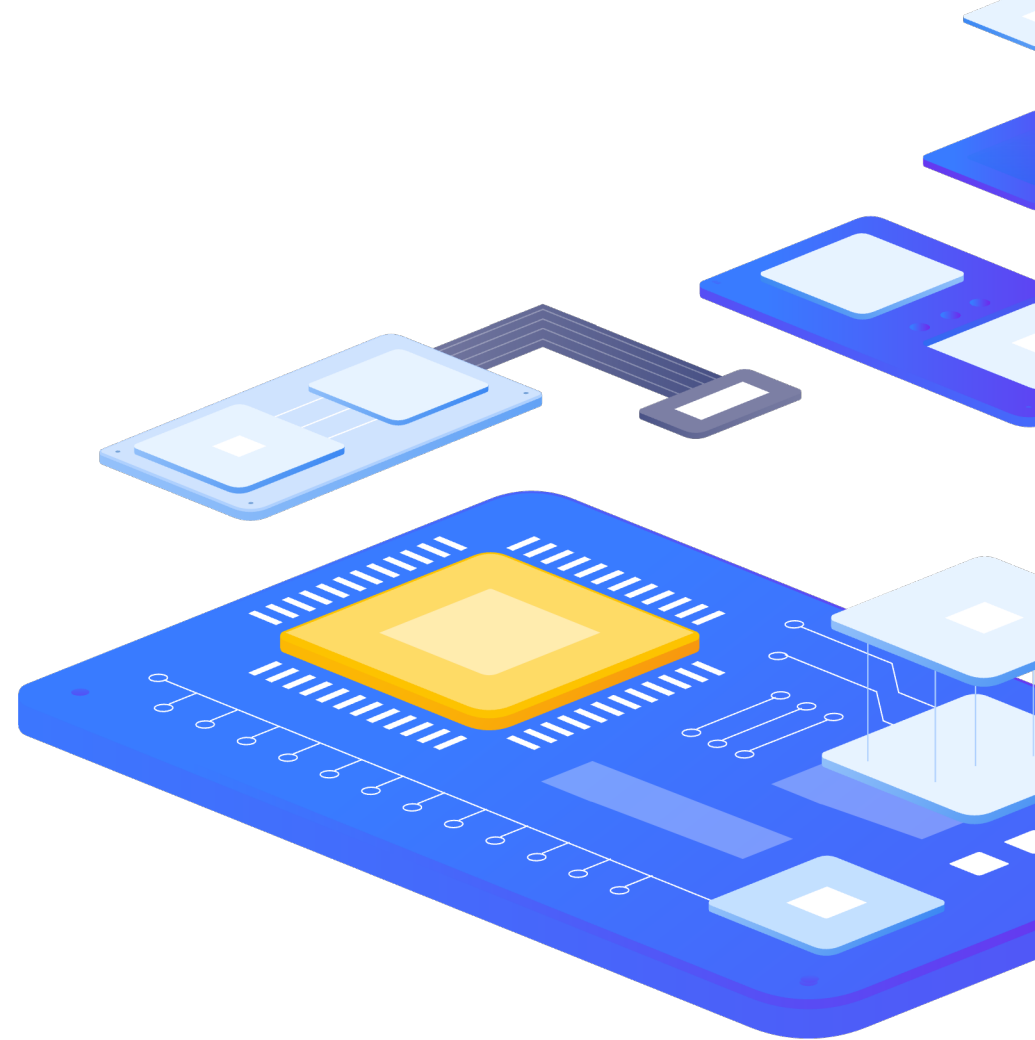
### SSH is not available

Problem definition:

› `max(/server/net.tcp.service[ssh],#3)=0`

Recovery expression:

› `min(/server/net.tcp.service[ssh],#10)=1`



## ADVANCED PROBLEM DETECTION

# Anomalies

### How to detect?

By comparing with the data from the same period, the period is taken from the past.

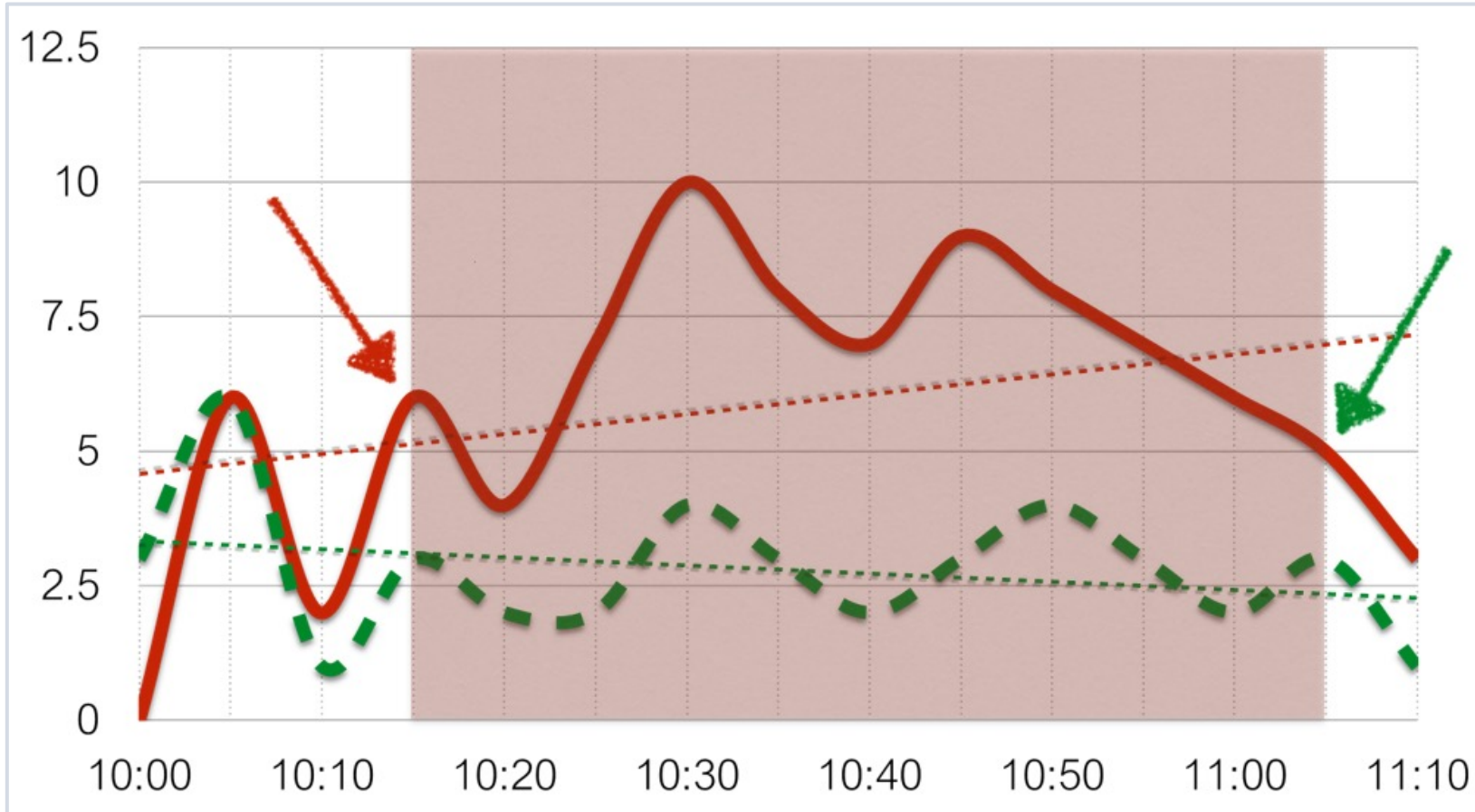
Average CPU load for the last hour is 2x higher than

CPU load for the same period week ago

▶ `avg(/server/system.cpu.load,1h) > 2* avg(/server/system.cpu.load,1h:now-1w)`

## ADVANCED PROBLEM DETECTION

# Anomalies

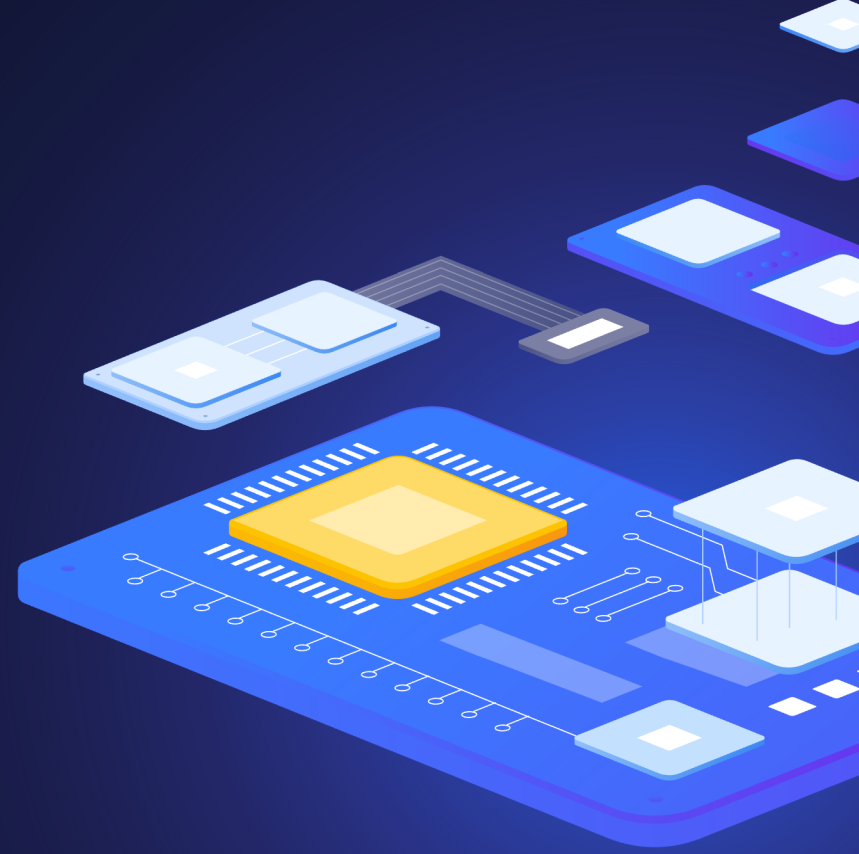


Comparison with the data 7 days ago



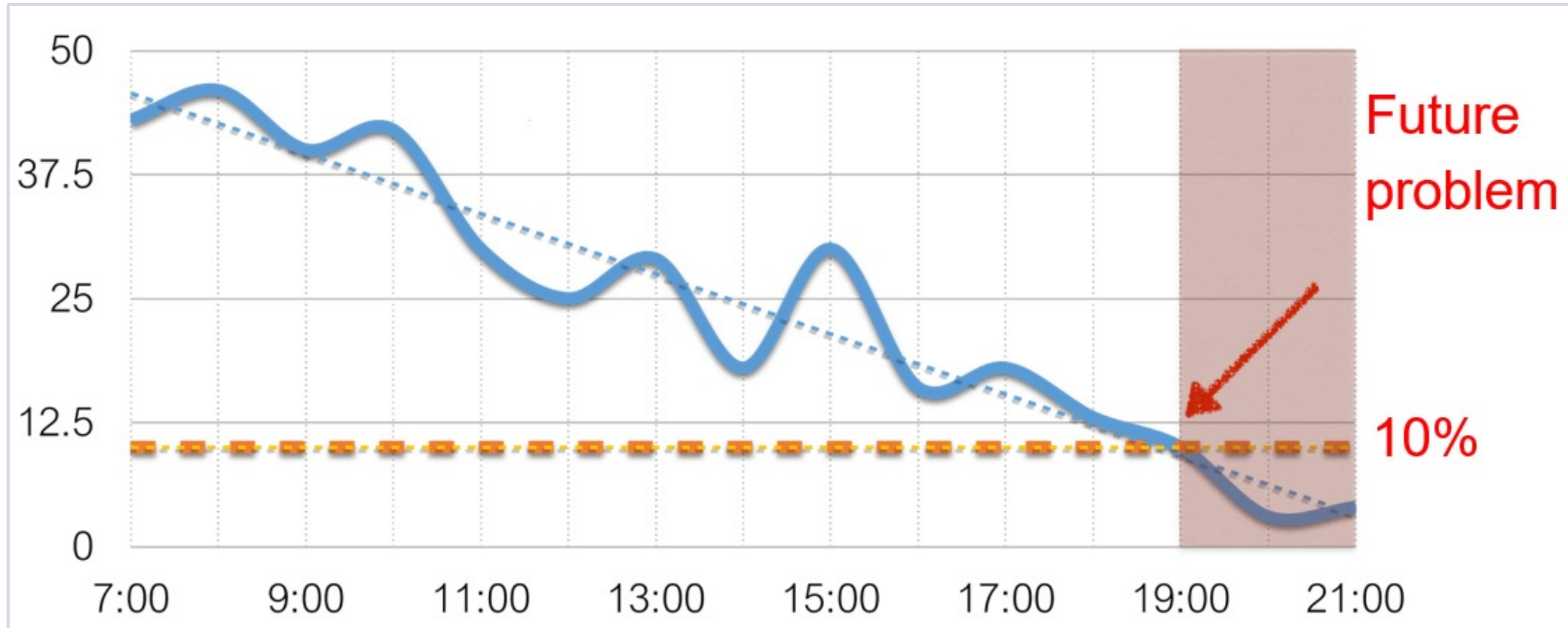
3

Forecast



## ADVANCED PROBLEM DETECTION

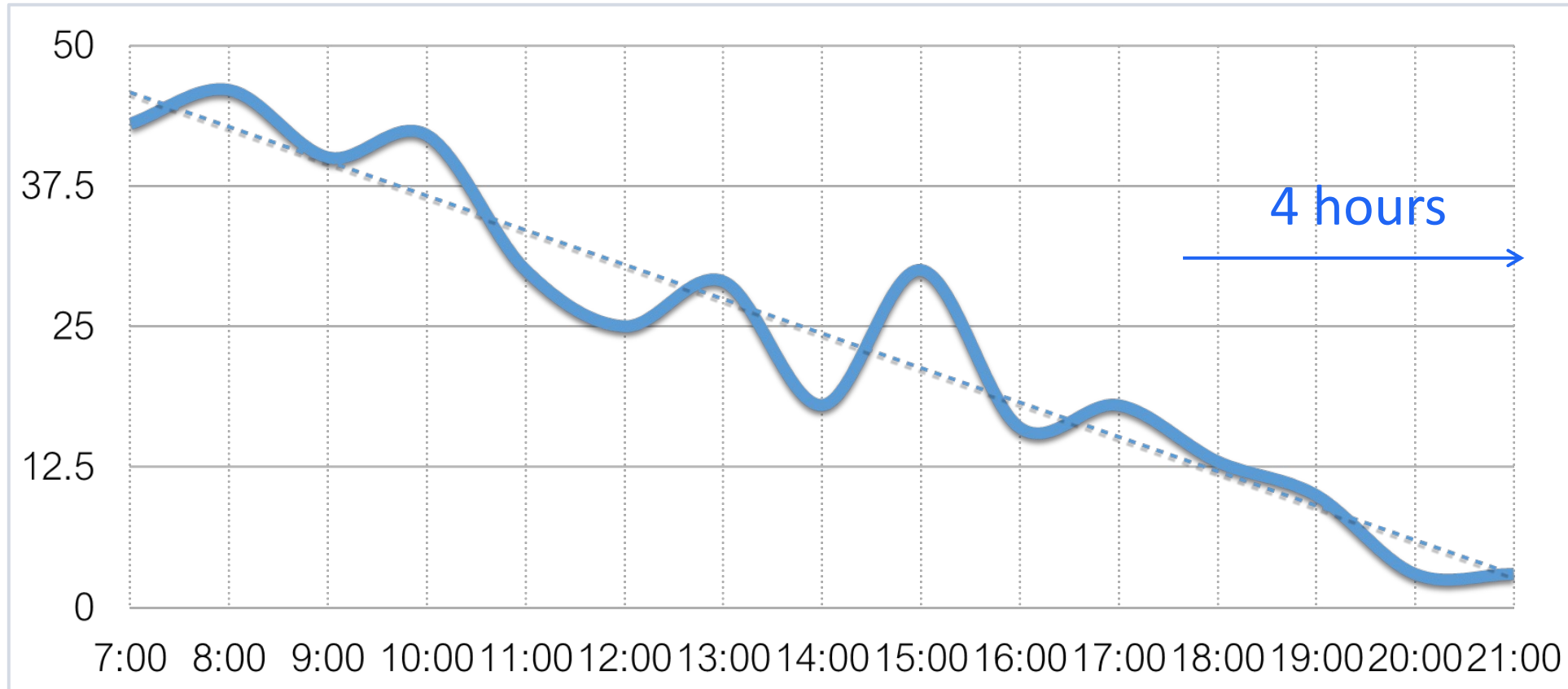
## Forecast



Trigger function timeleft

## ADVANCED PROBLEM DETECTION

## Forecast



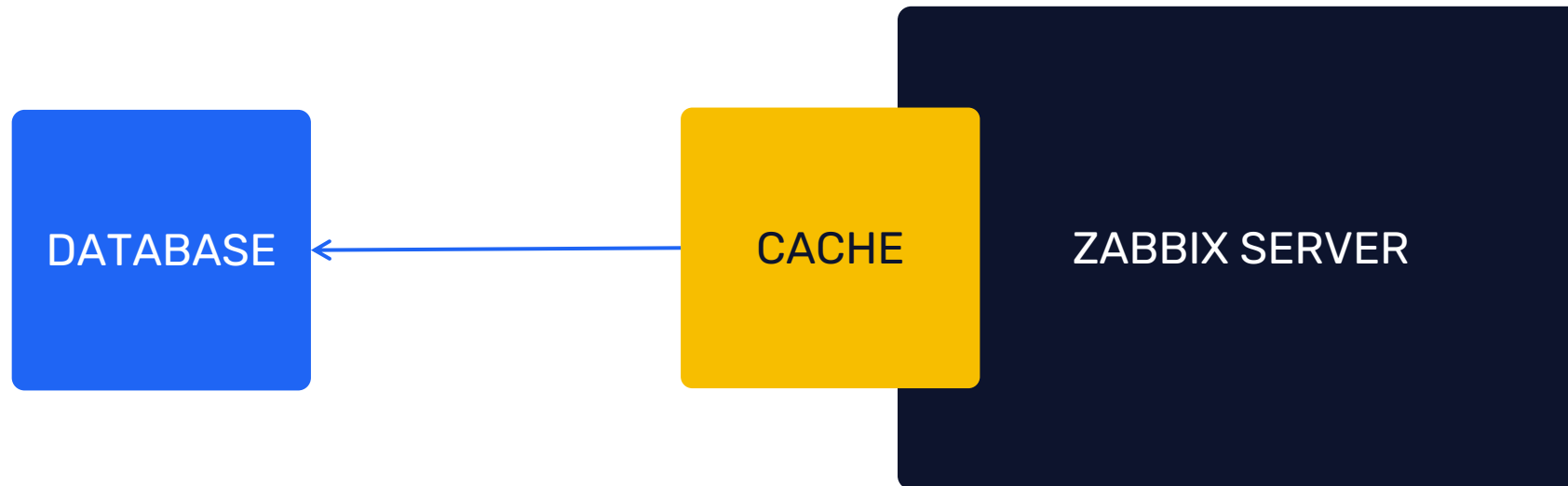
Trigger function forecast

## ADVANCED PROBLEM DETECTION

# Does history analysis affect performance of Zabbix?

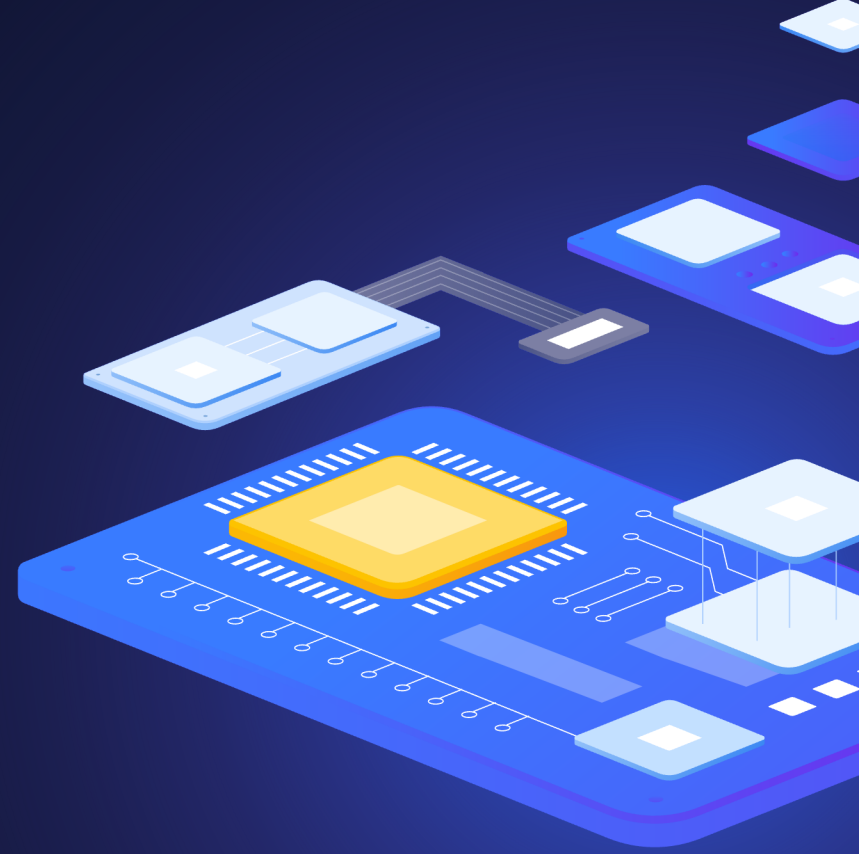
Yes, but not significantly.

Especially as of Zabbix 2.2.0.



4

# Dependencies



## ADVANCED PROBLEM DETECTION

# Dependencies

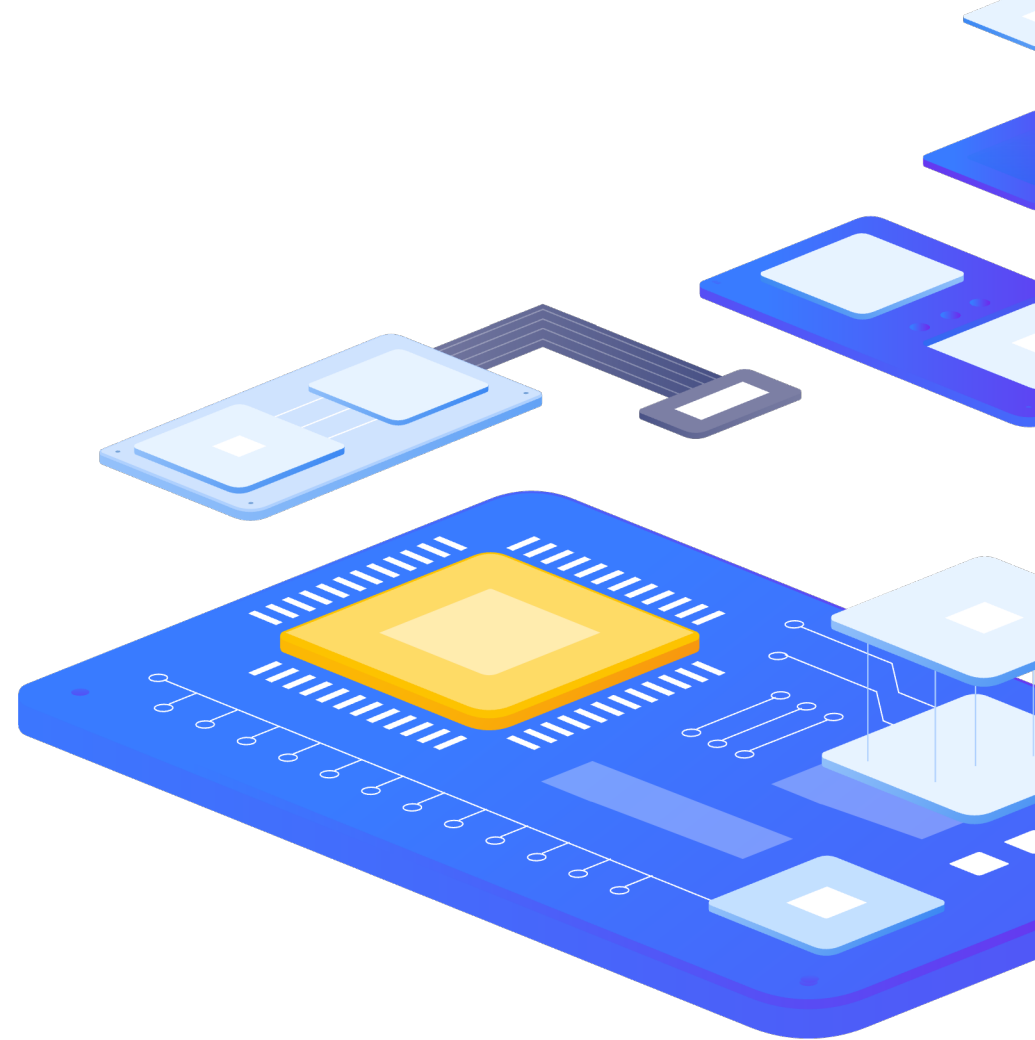
CRM is not working



DB is unavailable




No free disk space



# ADVANCED PROBLEM DETECTION

## Section „Problems“



Monitoring

Dashboard

Problems

Hosts

Latest data

Maps

Discovery

Services

Inventory

Reports

Configuration

Administration

Problems

Export to CSV

Filter

Show

Recent problems

Problems

History

Host groups

type here to search

Select

Hosts

type here to search

Select

Application

type here to search

Select

Triggers

type here to search

Select

Problem

type here to search

Select

Severity

☐ Not classified
 ☒ Warning
 ☒ High
 ☐ Information
 ☐ Average
 ☒ Disaster

Age less than

14

days

Host inventory

Type

Remove

Tags

And/Or

Or

tag

Contains

Equals

value

Remove

Show tags

None

1

2

3

Tag name

Full

Shortened

None

Tag display priority

comma-separated list

Show operational data

None

Separately

With problem name

Show suppressed problems

Show unacknowledged only

Compact view

Show timeline

Show details

Highlight whole row

Apply

Reset

5

Tags





# Tags

Tag word: meaning

*Customer:* Alza

*Customer:* Globus

*Datacenter:* NY2

*Datacenter:* San Francisco

*Area:* Performance

*Area:* Availability

*Area:* Security

*Environment:* Staging

*Environment:* Test

*User impact:* None

*User impact:* Critical

## ADVANCED PROBLEM DETECTION

# Use of obtained values

Use of useful information in tags or names

* Name	Free disk space is less than {\$LOW_SPACE_PCT_HIGH:"{#FSNAME}"}% on volur					
Event name	Free disk space is less than {\$LOW_SPACE_PCT_HIGH:"{#FSNAME}"}% on volume {#FSNAME}					
Operational data	{ITEM.LASTVALUE1} (Total: {ITEM.LASTVALUE2}, Free: {ITEM.LASTVALUE3})					
Severity	Not classified	Information	Warning	Average	High	Disaster
* Expression	<pre>last(/Template OS - Windows - za/vfs.fs.size[{#FSNAME},pfree]) &lt;{\$LOW_SPACE_PCT_HIGH:"{#FSNAME}"} and last(/Template OS - Windows - za/vfs.fs.size[{#FSNAME},total])&gt;=0 and last(/Template OS - Windows - za/vfs.fs.size[{#FSNAME},free])&gt;=0</pre>					Add
<a href="#">Expression constructor</a>						
OK event generation	Expression	Recovery expression	None			

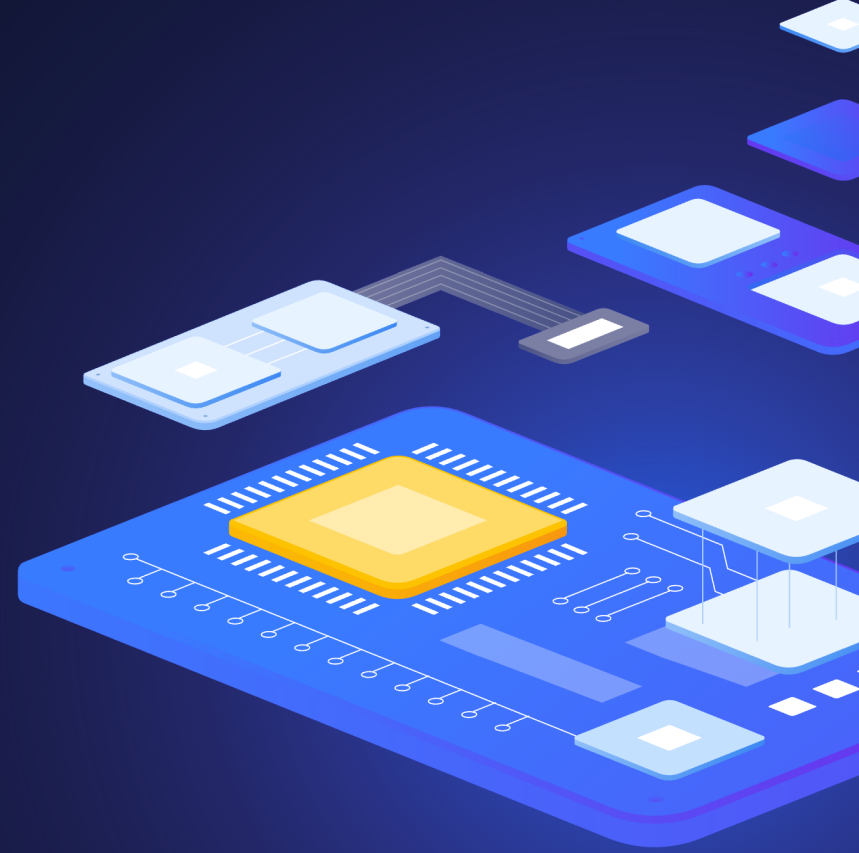
## ADVANCED PROBLEM DETECTION

# Possible reactions

- › Event correlation
- › Automatized problem solving
- › Manual problem closing
- › Sending notifications to a user or a group of users
- › Registration of tasks in the Helpdesk system

6

# Event correlations



## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

Trigger

Tags

Dependencies

\* Name

Service {{ITEM.VALUE}.regsub("^.\* service ([a-zA-Z]\*) .\*\$", "\1")} stopped

Event name

Service {{ITEM.VALUE}.regsub("^.\* service ([a-zA-Z]\*) .\*\$", "\1")} stopped

Operational data

Severity

Not classified

Information

Warning

Average

High

Disas

\* Problem expression

find(/My host/log[/var /log/syslog],, "regexp", "Stopping")=1

Add

Expression constructor

OK event generation

Expression

Recovery expression

None

\* Recovery expression

find(/My host/log[/var /log/syslog],, "regexp", "Starting")=1

Add

Expression constructor

PROBLEM event generation mode

Single

Multiple

OK event closes

All problems

All problems if tag values match

\* Tag for matching

Service

Correlation of events at the trigger level allows you to compare individual problems reported by a single trigger.

Trigger

Tags 2

Dependencies

Trigger tags

Inherited and trigger tags

Name

Value

Datcenter

value

Service

{{ITEM.VALUE}.regsub("^.\* service ([a-zA-Z]\*) .\*\$", "\1")}

Add

## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped

"Service Jira stopped"

PROBLEM

## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped      "Service Jira stopped"

PROBLEM

10/Feb/2022:06:27:32 service MySQL stopped      "Service MySQL stopped"

PROBLEM

## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"
10/Feb/2022:06:28:11 service MySQL started	

PROBLEM

RESOLVED



## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"	PROBLEM
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	"Service Redis stopped"	PROBLEM

## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"	<b>PROBLEM</b>
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"	<b>RESOLVED</b>
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	"Service Redis stopped"	<b>RESOLVED</b>
10/Feb/2022:06:37:58 service Redis started		

## ADVANCED PROBLEM DETECTION

# Event correlation on trigger level

How does it work?

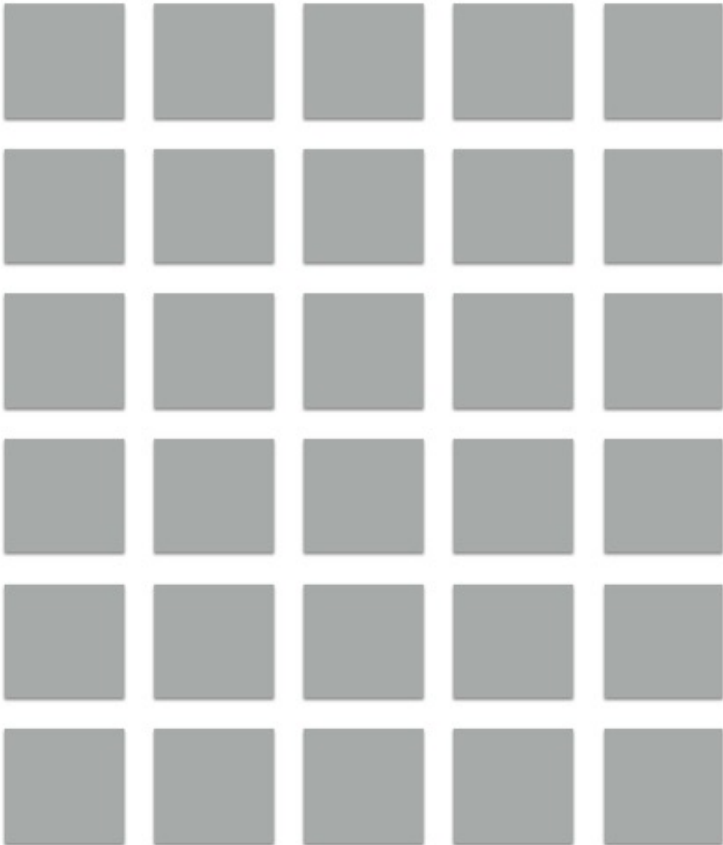
10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"	RESOLVED
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	"Service Redis stopped"	RESOLVED
10/Feb/2022:06:37:58 service Redis started		
10/Feb/2022:06:55:31 service <b>Jira</b> started		

# Event correlation

**A new problem appears**



**Existing problems**

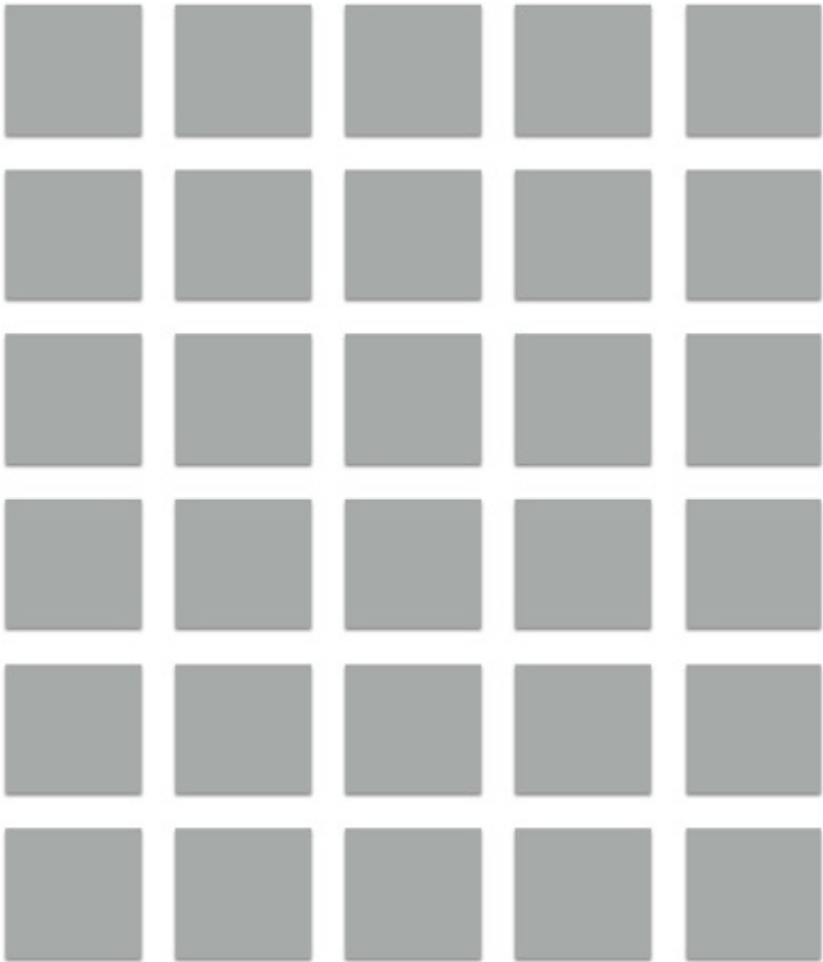


Correlation rules



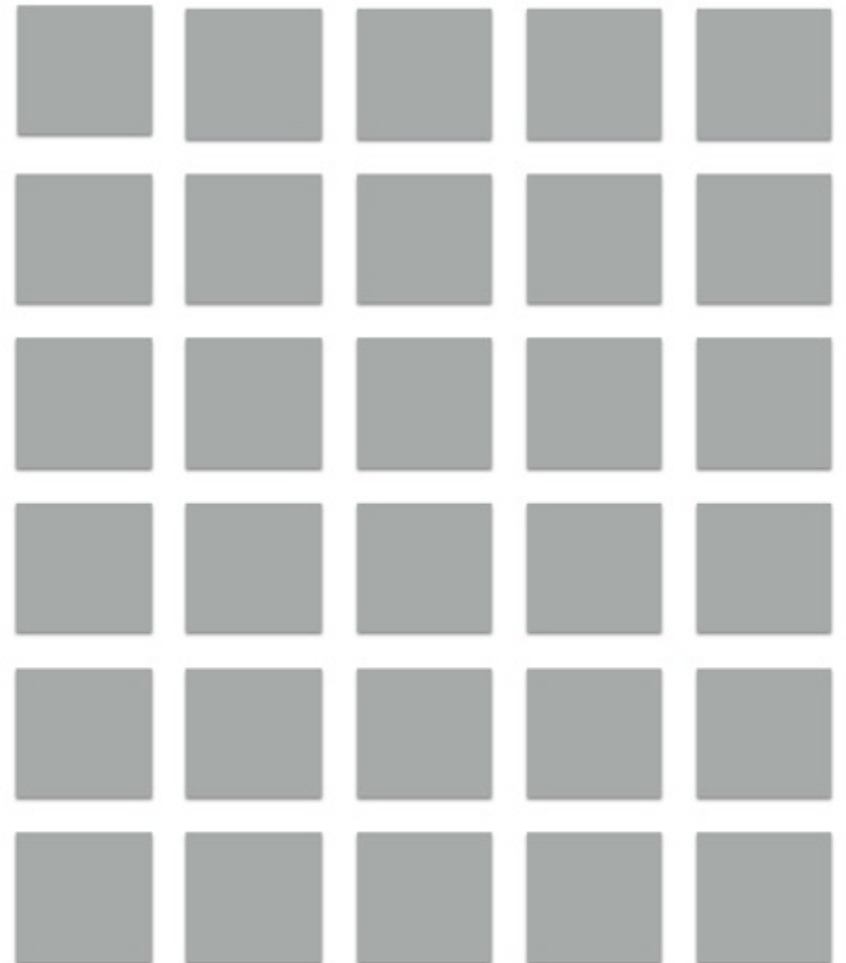
# Event correlation

**Existing problems**



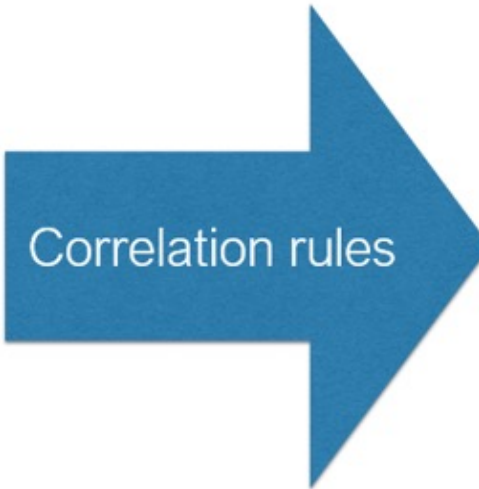
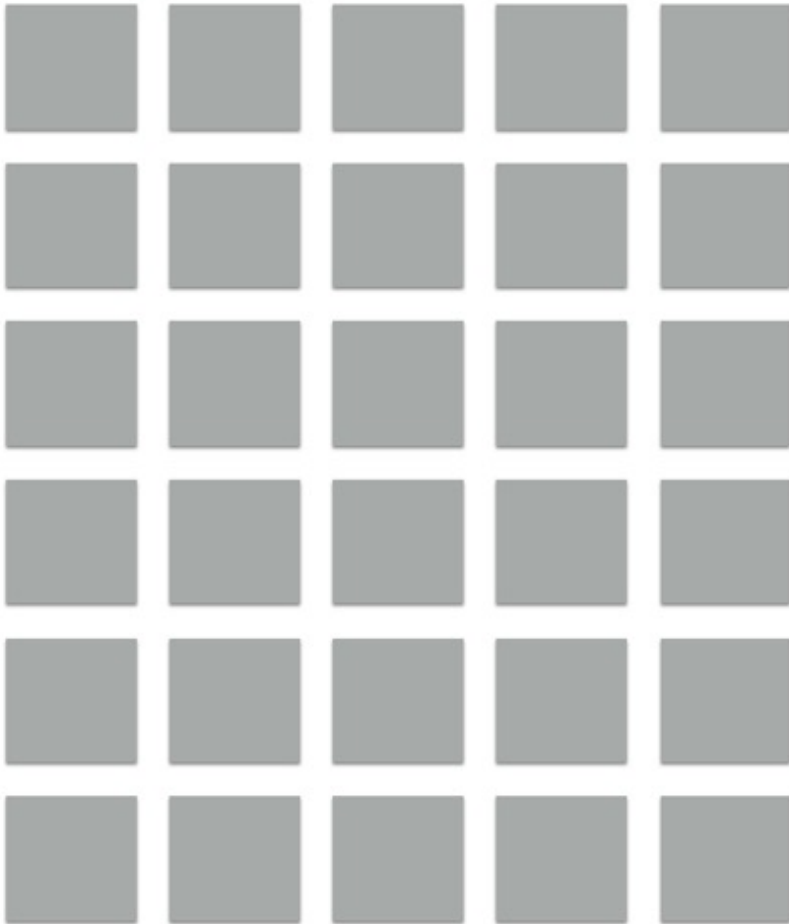
Correlation rules

**No correlation rules**

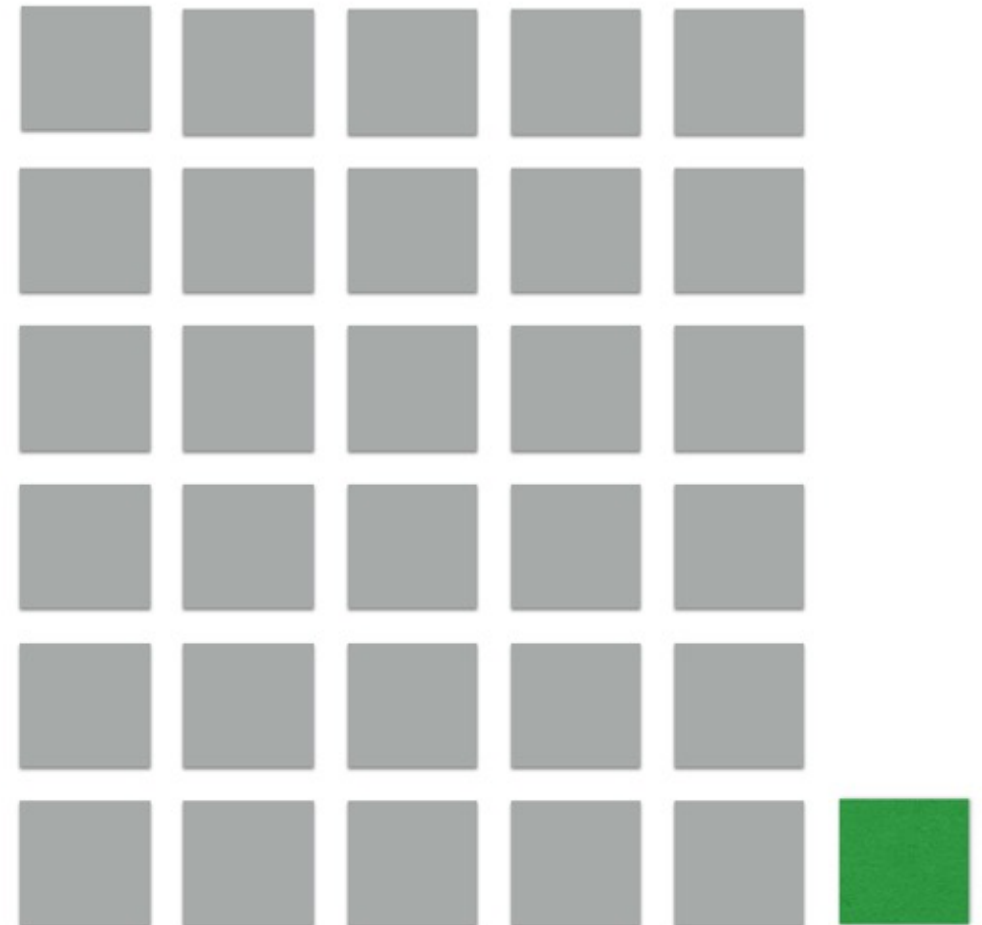


# Event correlation

## Existing problems

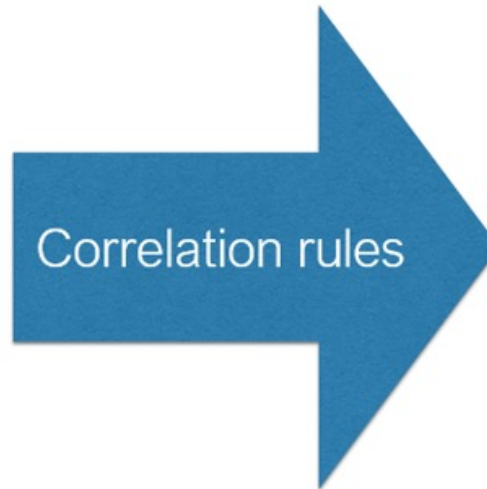
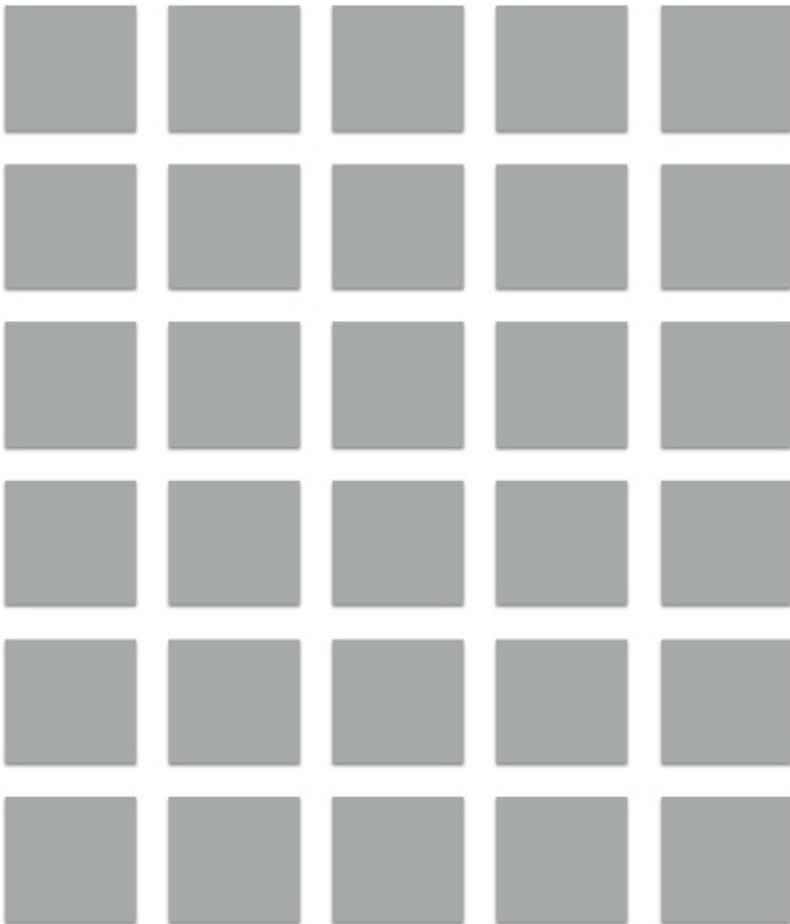


## No correlation rules

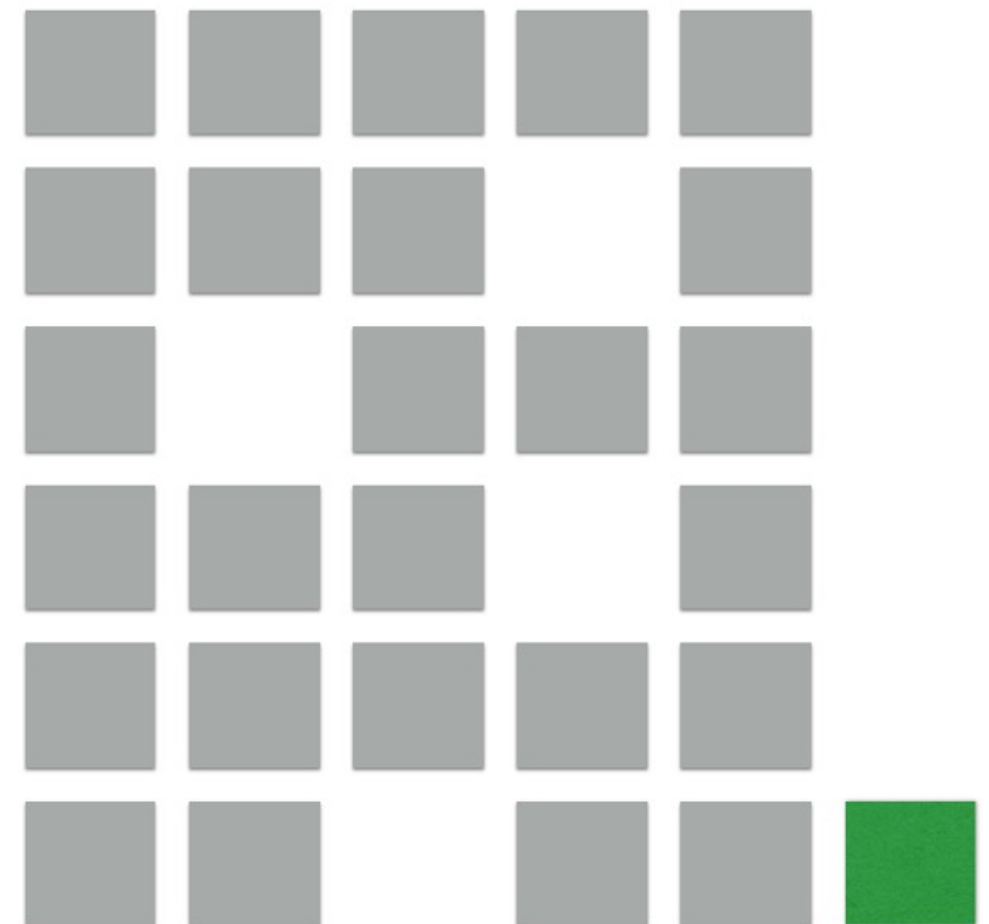


# Event correlation

## Existing problems



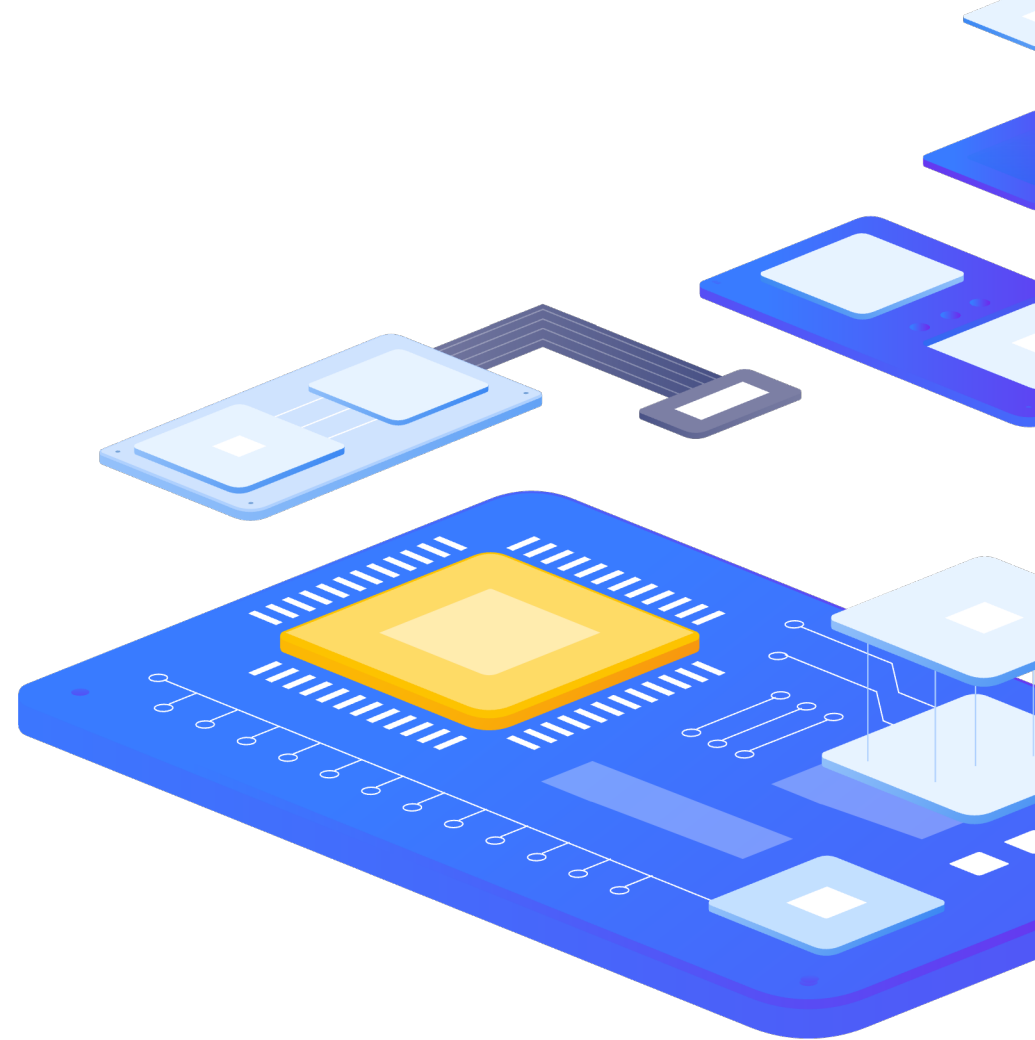
## No correlation rules (close



## ADVANCED PROBLEM DETECTION

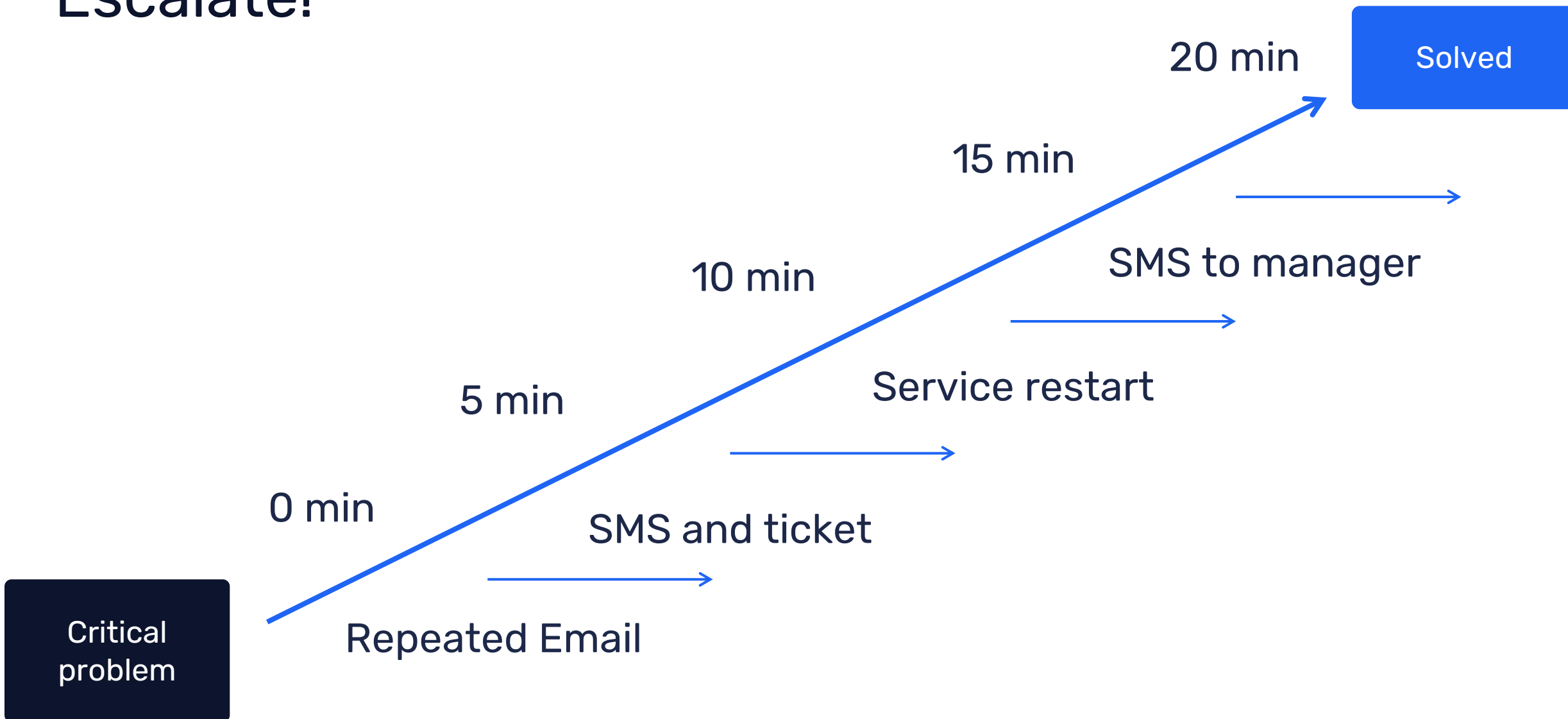
# Escalate!

- › Immediate reaction
- › Delayed reaction
- › Notification if automatic action failed
- › Repeated notifications
- › Escalation to a new level





# Escalate!



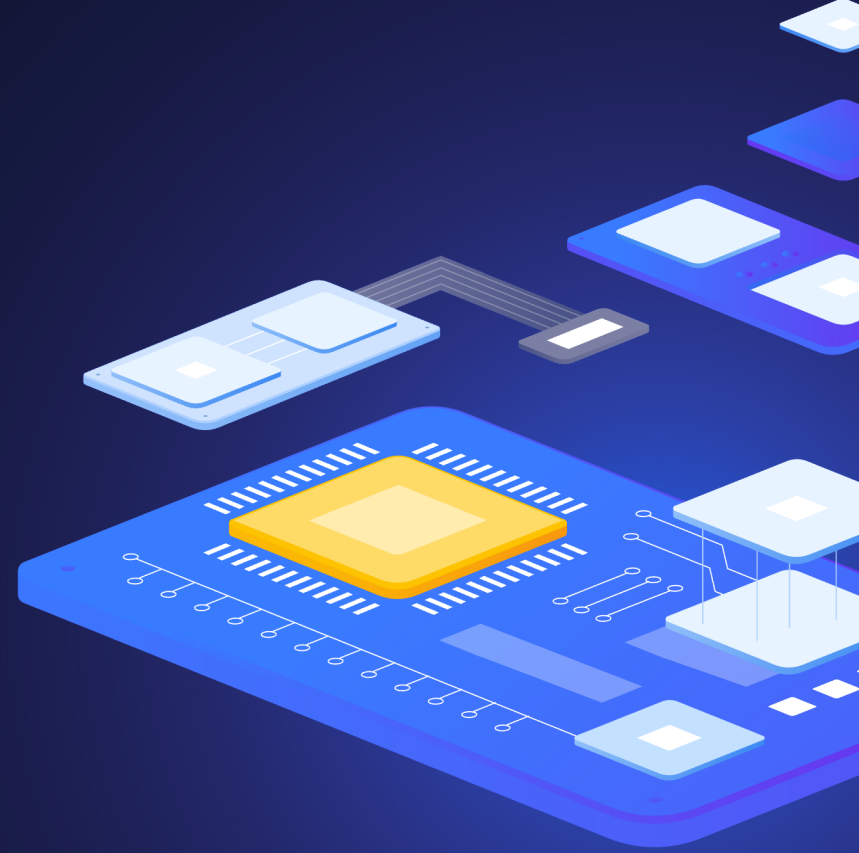
## ADVANCED PROBLEM DETECTION

# In summary

- › Analyze history
- › No problem!= Solution
- › Use different conditions for problem definition and recovery
- › Pay attention to anomaly detection
- › Use correlation
- › Resolve common problems automatically
- › Do not hesitate to escalate!

7

Expression macros



## ADVANCED PROBLEM DETECTION

# {?EXPRESSION\_MACROS}

- › If defined, this name will be used to create the problem event name, instead of the trigger name.
- › The event name may be used to build meaningful alerts containing problem data
- › The same set of macros is supported as in the trigger name, plus {TIME} and {?EXPRESSION} expression macros.
- › Supported since Zabbix 5.2.0
- › Can be used in different locations – **Event Name**, Maps, name of Graphs

## ADVANCED PROBLEM DETECTION

# {?EXPRESSION\_MACROS}

### Junior

- › Problem: Load of **Exchange** server increased by more than 10% last month

### Expert

- › Problem: Load of **Exchange** server increased by **24%** in **July (0.69)** comparing to **June (0.56)**
- › Load of {HOST.HOST} server increased by
  - › {{?100\*trendavg(//system.cpu.load,1M:now/M)/trendavg(//system.cpu.load,1M:now/M-1M)}.fmtnum(0)}}% in
  - › {{TIME}.fmttime(%B,-1M)}
  - › ({{?trendavg(//system.cpu.load,1M:now/M)}.fmtnum(2)}} comparing to
  - › {{TIME}.fmttime(%B,-2M)}
  - › ({{?trendavg(//system.cpu.load,1M:now/M-1M)}.fmtnum(2)}})

<https://www.zabbix.com/documentation/6.0/en/manual/config/triggers/expression?hl=expression#examples-of-triggers>

8

Demo



9

Questions



# CONTACT US:

Phone:



+420 800 244 442

Web:



<https://www.initmax.cz>

Email:



[tomas.hermanek@initmax.cz](mailto:tomas.hermanek@initmax.cz)

LinkedIn:



<https://www.linkedin.com/company/initmax>

Twitter:



<https://twitter.com/initmax1>

Tomáš Heřmánek:



+420 732 447 184