



Compose IT



# Get more out of NOI

IBM usergroup Nordics 2021

# Event Management – the origin of NOI

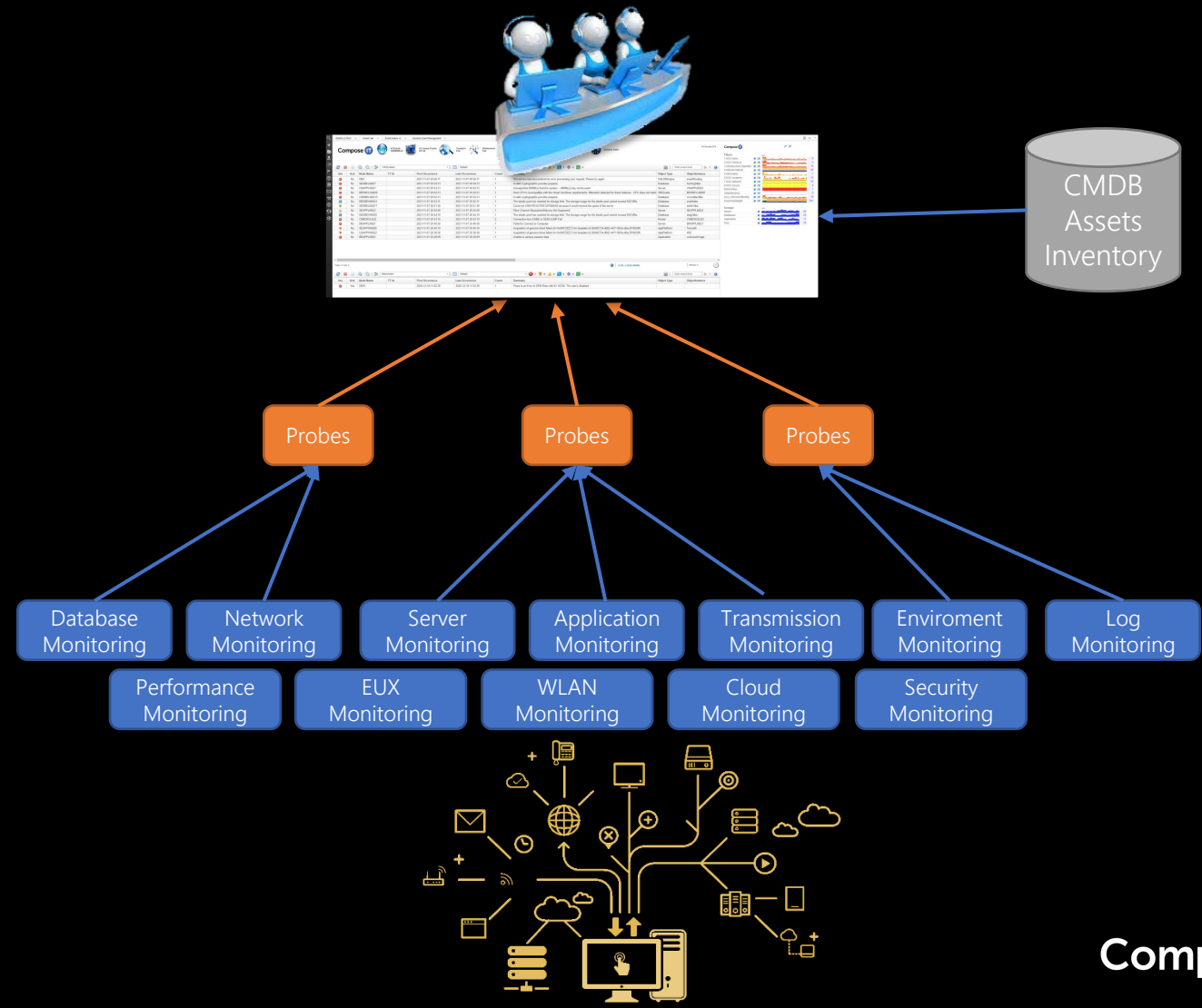
- The ability to collect any events from any source to one system.
- Events are normalized and deduplicated
- Events are enriched with context from CMDB/ Assets/Inventory

This gives:

- All alerts on One screen.
- All events look the same
- One tool to learn, not 12

Now it's possible to:

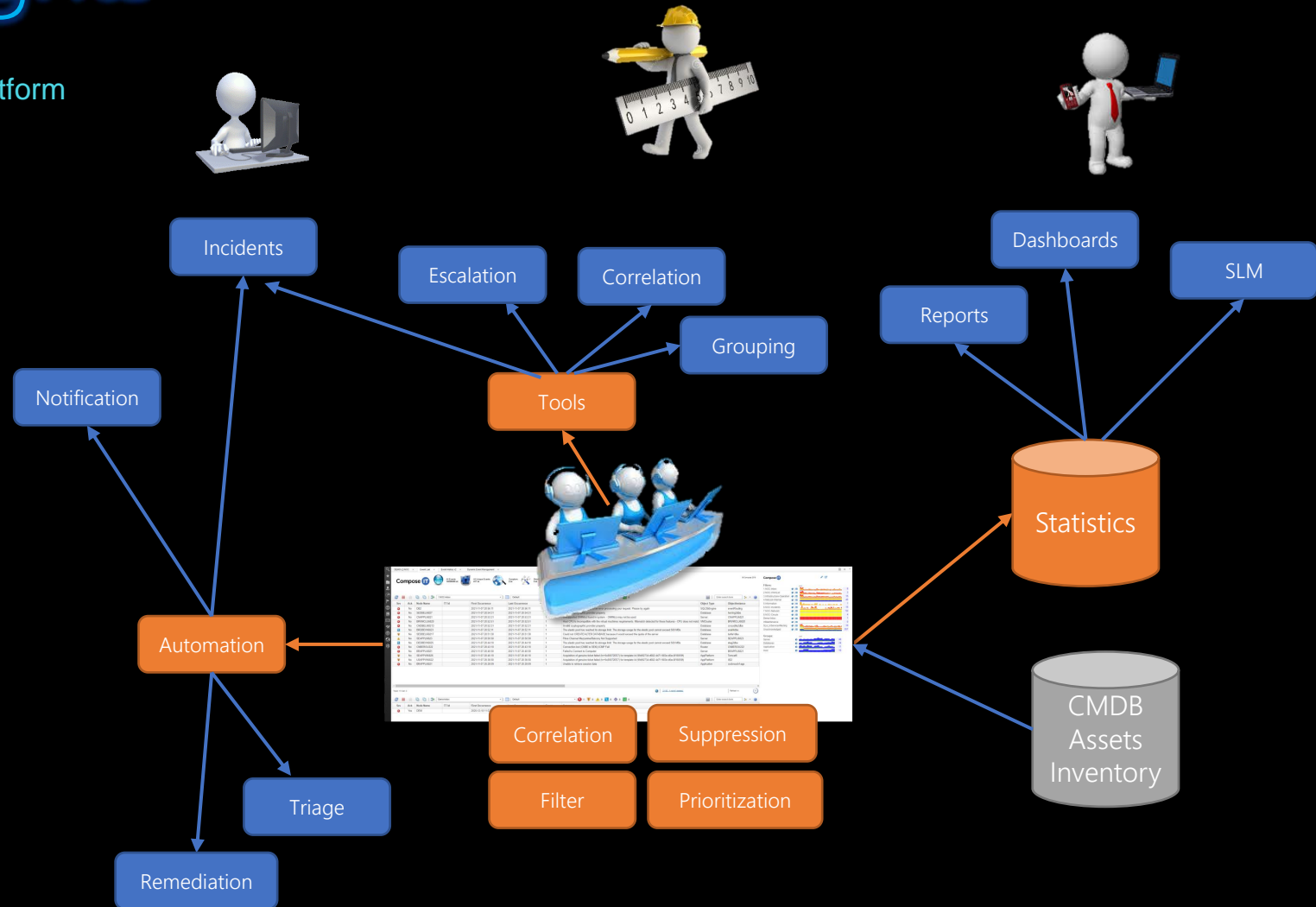
- Prioritize & Filter
- Analyze & Correlate
- Integrate & Automate
- Escalate & share





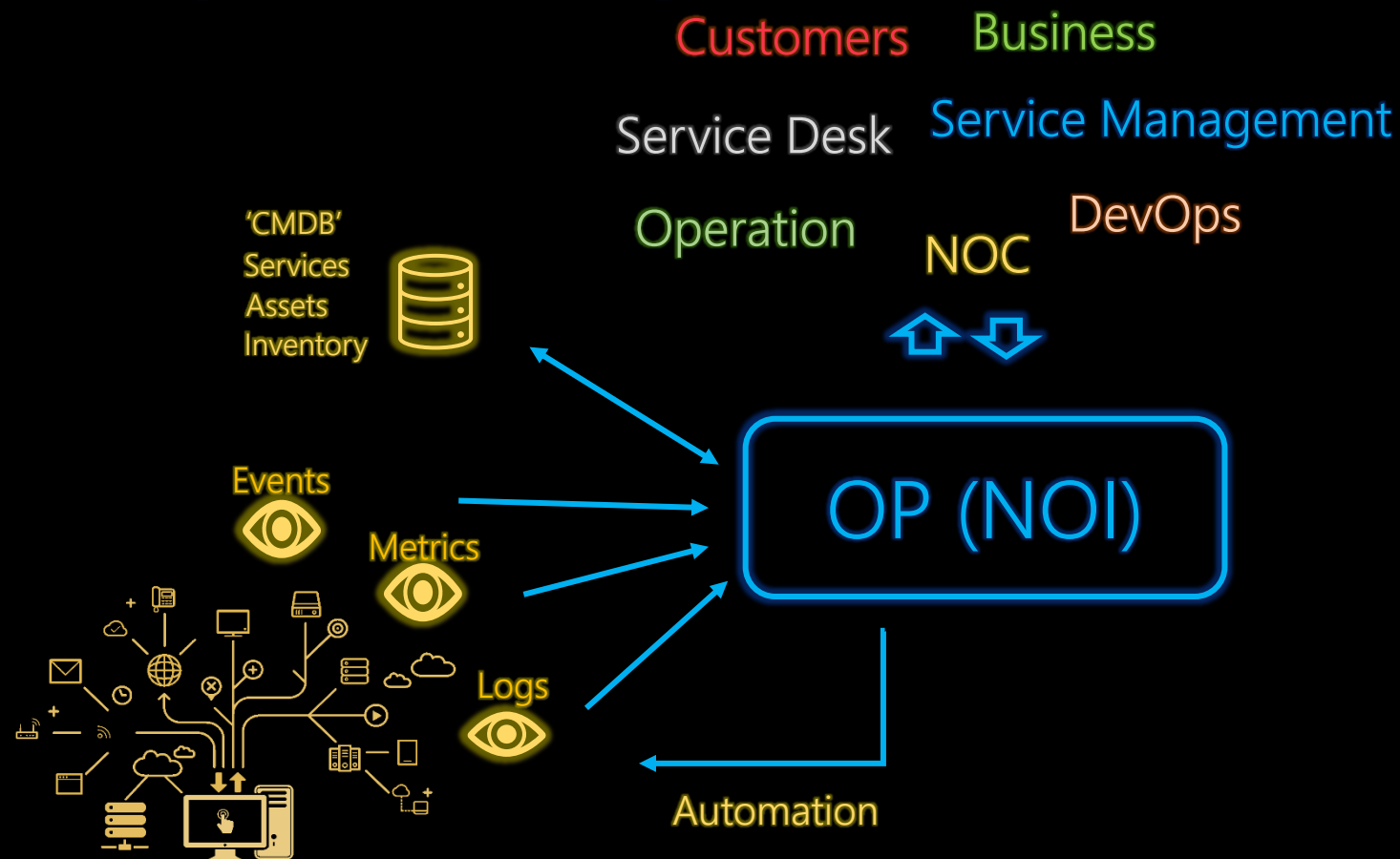
# Operational Insights

- With this normalized data, it becomes a platform for:
- Event suppression by:
  - Correlation
  - Filters
  - Prioritization
  - Change suppression
- NOC can:
  - Escalate
  - Create Incidents
  - Make manual correlations & group-events
- Automation to:
  - Notify & create incidents
  - Escalate
  - Run Triage
  - Correlations & group events
  - Run remediations
- Statistics to:
  - Run reports
  - Drive Dashboards
  - Integrate to Service Level Management



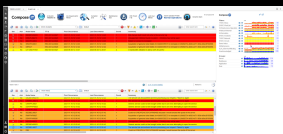
# Challenges for an Operation platform?

- Ever changing environments
- Changing operational model
- Correct operational information
- TTM (Time to market)
- Different OLA/SLAs
- Less resources
- Different demands from different consumers



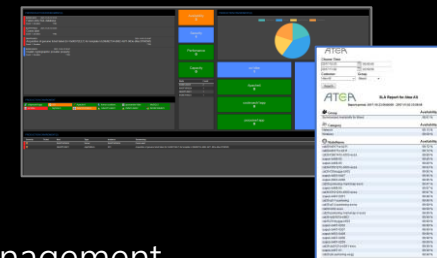
# Typical demands

It's all based on 'filters',  
in one way or another



Operation Center

- Tools to manage events
- Group events
- Filter & Views
- Correlations
- Automations



Service Management

- How is my service doing?
- How is customer X performing?
  - Reports
  - Dashboards



- Search and filter
- Overview and context
- History reports
- "my " stuff
- Different ecalations in diffrent teams.

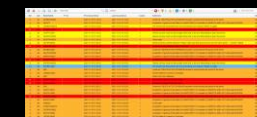
2nd line operation,  
3d line teams,  
DevOpsTeam



NOI

Event/Monitoring team

- How do we manage millions of events?
- How do vwe fullfill all different requirements?



- Manage new sources
- Controll that the right events goes t the right reciver

# Goals for a more efficient Operation Platform

## 1. Easy to add new sources/environments

- Possible to add new sources without affecting way of working reports or dashboards (keep filter and views intact)
- Structured and a defined way to add new environments



- Attribute Data Model
- Define incoming events (Event Classification)

## 2. Easy to manage events

- No technical skill to change event behavior
- Known effect when changing specific attributes



- GUI for attribute management (Dynamic Event Management)

## 3. Flexible

- Allow for development of new WoW (Way of working)
- Support multiple wow at the same time (IT-Ops, DevOps, Infra, Application, ...)



- Dynamic escalation (action) rules to route alerts

## 4. Quick to meet new demands

- Easy to create new filters and views
- Fast & easy to set up new dashboards
- Easy to search and export information
- Easy to develop new features



- Drag n drop dashboards
- Flexible search/history

Classify incoming events and set attributes that makes filters easy and flexible!



# Event classification

- **Event source certification:**

- Rulefile and DynamicEventManager**

- Minimize Rulefile configuration and allow non experts to administrate Event Certification and event normalization.

- A defined process to add new sources and certify events gives an efficient solution.

- **Event normalization:**

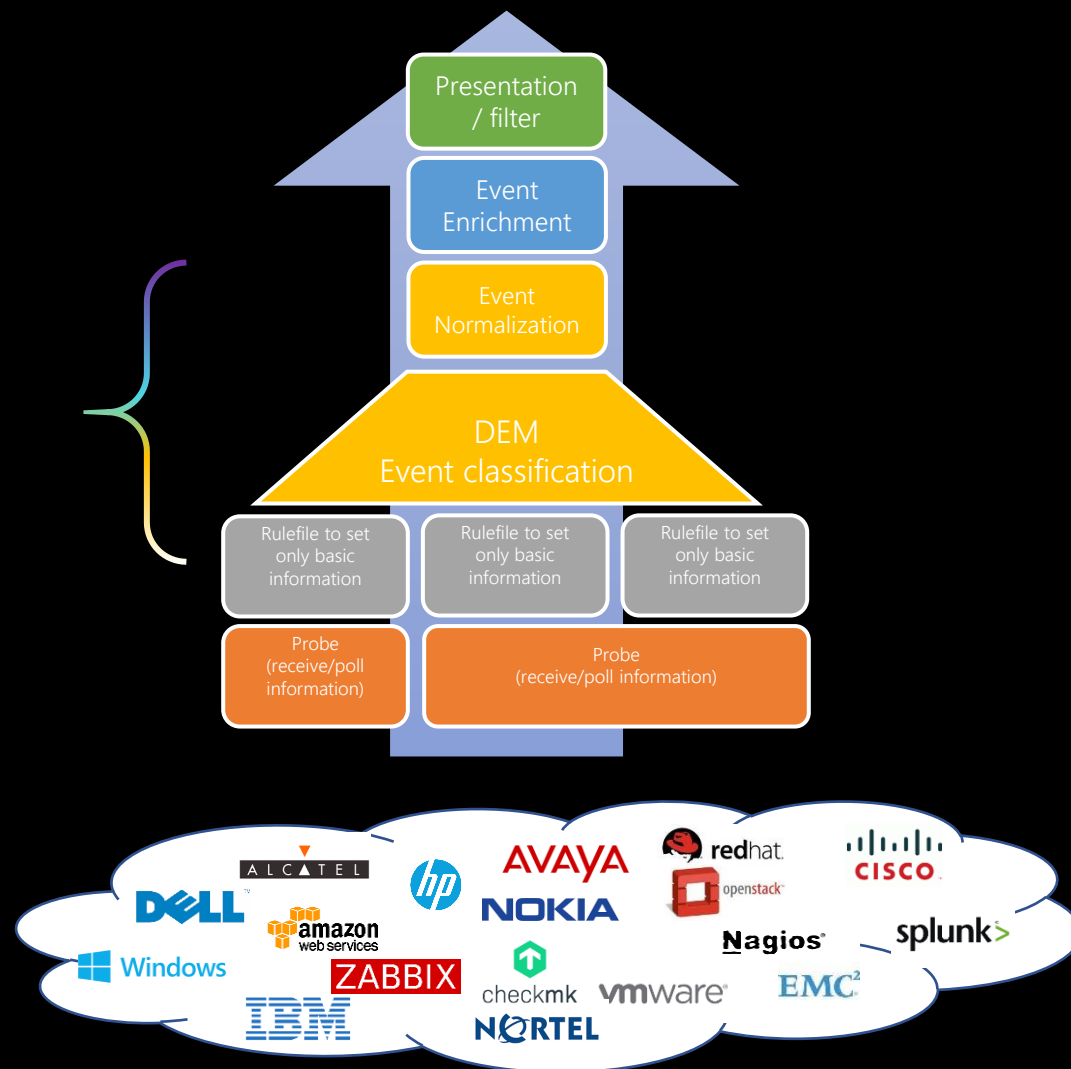
- Set attributes: ObjectType, KPI, ServiceAffecting, Actions**

- By utilizing standardized attributes like ObjectType and KPI together with automated triage-actions and service information events from different sources can be managed by the operation processes with minimal adoption or disruption.

- **Flexible source differentiation and multidomain support**

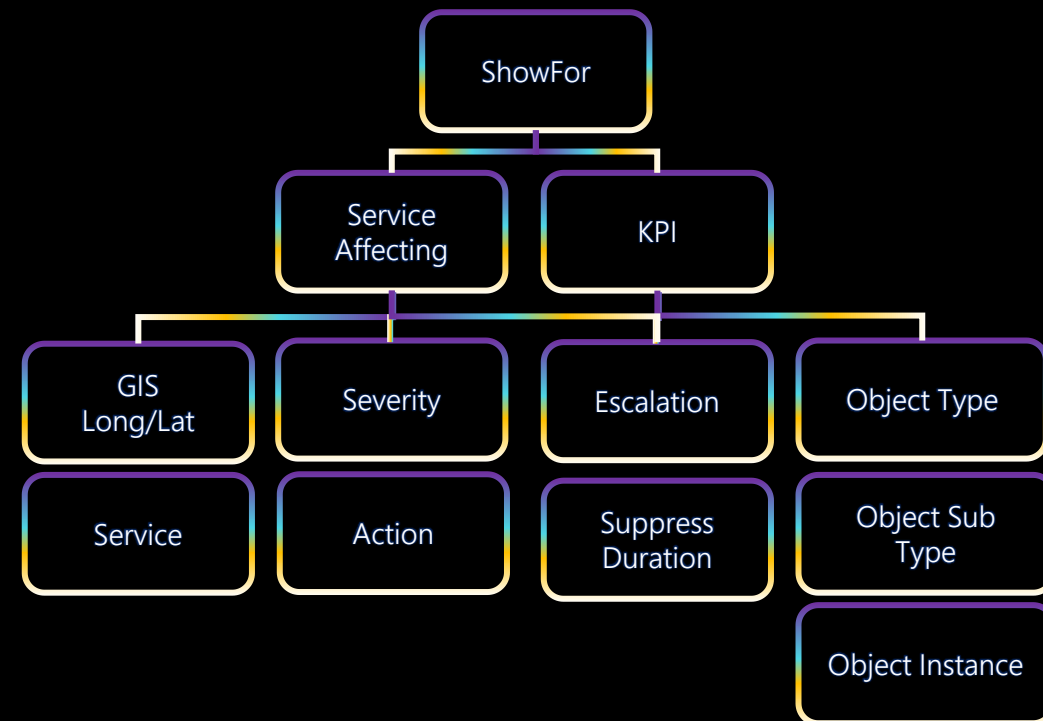
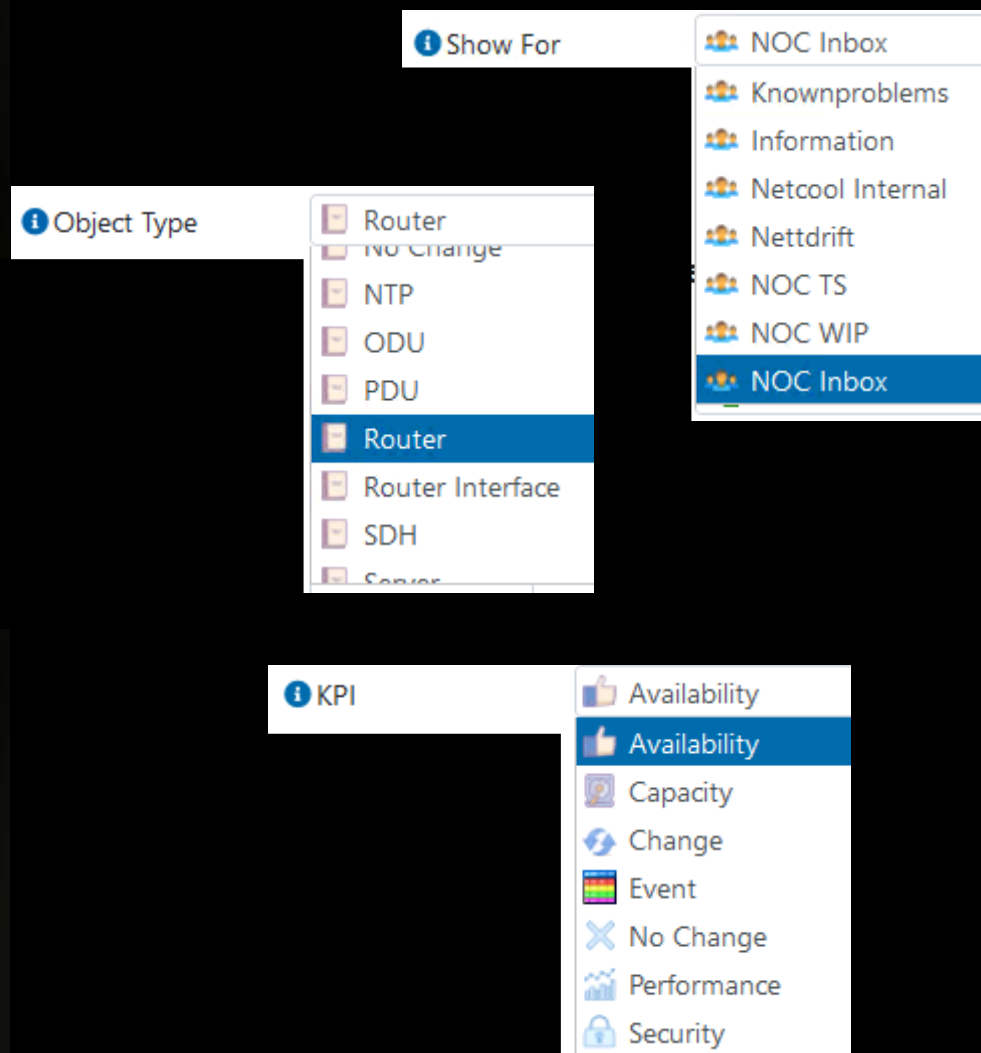
- (DEM and Netcool architecture )**

- The layered approach gives a flexible solution that can adopt to many different sources and technologies and still present and interact with the operational process in a homogeneous way.





# Attribute data model



The datamodel is defined fields in the Omnibus to let you classify and manage how the event will be displayed or if any action should be automated.

With the data model you can have simplified filters and focus on *Event Classification*.

This will ensure that the right events are visible to the right consumer regardless if it is consumed in reports, dashboards or event lists.

# 'EMPTY INBOX' CONCEPT (@Show For)

What we mean with empty inbox is literally that anything you see in the event list is something that need attention, an action.

To give an example of rule can be.

An event that indicate communication issue with a device, but from experience we know that we should not act within 30 minutes, so instead of letting the operator "remember" when an event is occurring and remember to check after 30 minutes we HIDE the event and if it's still communication issue after 30 minutes then it will be shown in the Inbox for the operator.

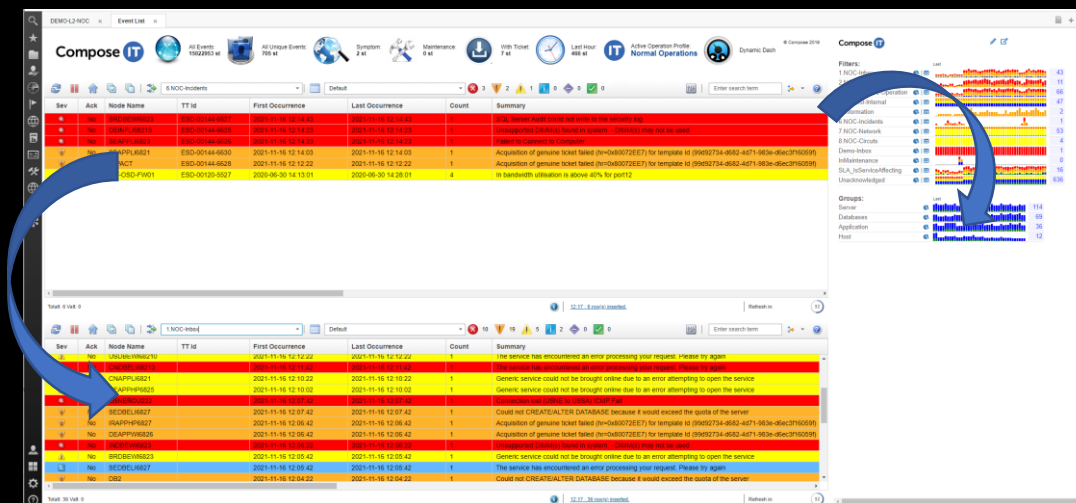
Or

You want an event to be shown for the Operation Center if the disk in volume C: is full, but not for other volumes an 'early warning' should be automatically be created to the application teams

This type of rules are configured in Dynamic Event Management, DEM and should be managed by Operation and the Netcool operation team to continuously improve the event/alert quality. The way of working is described in the “Event Certification process”

@ShowFor=12 (inbox)

@ShowFor=10 (WorkList)



```
@ShowFor >= 10
```

# Dynamic Event Management

- Defined Data model and triggers
- Event Matching with single or combinations of keys and timeframes
- GUI based Event Classification
- Show For logic - *Only show events that you expect someone to take care of*
- Event Enrichment - *Severity, ObjectType, Service Affecting, KPI etc.*
- Ticket Routing in ITSM system
- Event Actions - *Mail, SMS, Ticket, Delay, Escalation, Discard, Expire*
- Automation - *Database and Script based if-then-else logic for error isolation, triage and resolution*
- Group Correlation - *Different events from different sources can be correlated to a more important event*
- Reclassification - *Let the event be reclassified in a specified timeframe or XinY logic*
- On Duty Management - *Handle automatic event forwarding to duty groups by duty schedules*

The image displays two screenshots of the Compose IT Dynamic Event Management software. The top screenshot shows the main configuration interface with sections for Rule Information, Fault Management, Ticket Management, and Service Management. The bottom screenshot shows a detailed view of a rule configuration, including a table of event data and a flowchart diagram illustrating the event processing logic.

# Dynamic Event Management



DEMO-L2-NOC x Event List x Dynamic Event Management x

**Compose IT**

Instance: Production  
Rule Group: Choose Rule Group... Source: Choose Source... EventID:  Node:

Show Selected Show All

Show 15 entries

Export to Excel Export to CSV

Search:

Function	ID	Enabled	Source	EventID	Rule Name	Sub Source	Node	SQL Match	Operation Profile	Timebased rule	Severity	Show For	Object Type	KPI	Discard	Incident	Duty	Event Delay	Escalate	Time Window	Time Threshold	eMail	SMS	No Ack	Request	Teams	Serv
	45434		GenerateRandomTestDataV2	SystemBoadFailure		Any	Any	No Filter	Any			NOC SystemTekniker	ServerHardware					0	0	0	0						
	47813		Any	TestRule		Any	Any	No Filter	Any			No Change	Omnibus					0	0	0	0						
	45330		GenerateRandomTestDataV2	TheelasticpoolhaschedissoagelimiThesoageusagefoheelasticpoolcaex...		Any	Any	No Filter	Any			NOC Inbox	No Change					0	0	0	0						
	45415		GenerateRandomTestDataV2	ThesevemaivefailedisymbaeySomeofguaisoiselismayhavebeeload...		Any	Any	No Filter	Any			No Change	No Change					0	0	0	0						
	45327		GenerateRandomTestDataV2	ThesevicehascoeuedaeopocessigyoequesPleaseyagai		Any	Any	No Filter	Any			NOC Inbox	SQLDbEngine					0	0	0	0						
	45501		Netcool	TopClasses		Any	Any	No Filter	Any			Netcool Internal	Probe					0	0	0	0						
	45502		Netcool	TopNodes		Any	Any	No Filter	Any			Netcool Internal	Probe					0	0	0	0						
	45507		Netcool	TriggerStatus		Any	Any	No Filter	Any			Netcool Internal	Omnibus					0	0	0	0						
	45393		GenerateRandomTestDataV2	Uablecoeivesessiodaa		Any	Any	No Filter	Any			NOC Inbox	No Change					0	0	0	0						
	45341		GenerateRandomTestDataV2	Ukow		Any	Any	Yes	Any			No Change	No Change					0	0	0	0						
	45360		GenerateRandomTestDataV2	UsuppoedDIMMsoudisysen-DIMMsmaeybeused		Any	Any	No Filter	Any			NOC Inbox	No Change					0	0	0	0						
	45497		Netcool	WebGUI Status		Any	Any	No Filter	Any			Netcool Internal	OmnibusWebGUI					0	0	0	0						
	45400		GenerateRandomTestDataV2	WebSieDOWN		Any	Any	No Filter	Any			No Change	No Change					0	0	0	0						
	47688		Undefined	[Backup-Check-Application][Error]		Any	Any	No Filter	Any			No Change	Backup					0	0	0	0						
	47689		Undefined	[Backup-Check-Application][Success]		Any	Any	No Filter	Any			No Change	Backup					0	0	0	0						

Showing 76 to 90 of 95 entries

Previous 1 2 3 4 5 6 7 Next



Rule Added/Changed by: nh 2018-10-02 10:24 Last Seen: 2021-11-16 21:21 Total Tally: 61341

☒ Rule ☐ Timebased rule☒ Instance ☐ Valid

## Event Information

☒ Production

☐ Invalid

Timeframe: Hourly

Start time: HH:mm

Stop time: HH:mm

Rule Name: Enter a name to the rule (optional)

Source: GenerateRandomTestDataV2

EventID: clusevicehasdeemiedhahisodedoesohavehelaescopyofclusecfiguaiodaa

Sub Source: Any

Node: Any

SQL Match: No Filter

Operation Profile: Compose IT Normal Operations

## Fault Management

Severity: Critical

Show For: NOC Inbox

Duty: Yes

Duty Group: Test

Summary: \*\*HighPrio\*\*

## Ticket Management

Support Group: No Change

Support Type: Server.OS

Sub Type: Linux

Module: No Change

Template: Infrastructure

Sub Module: No Change

Error Code: No Change

## Knowledgebase Connect

KB Source: Infrastructure

KB Article: Cluster resource failed

KB Group: Server

KB Sub Group: Linux

## Service Management

Object Type: Linux

KPI: Availability

Service Affecting: Yes

Service: No Change

BSM Identity:

## Event Action

ReClassification: Based on...

Time Threshold: 0 events

Event Delay: 0 min

Escalate: 0 min

SNMP Set:

Discard: ☐

eMail: ☐

SMS: ☐

Incident: ☒

No Ack: ☐

Request: ☐

Jira: ☐

Automation: ☒

Automation: Check Availability

View Scenario

# Automation

- If-then-else logic
- Custom scripts
- Update to events
- Clear events
- Escalate events

**Add/Change Automation**

Scenario: CHECK WINDOWS SERVICE

Scenario description: Scenario that uses JUMPHOST to access Windows hosts to check status of service and startup settings

**Add new item to the topology**

Parent: Host Reachability

Name:

Result equals: ==

Script name: --Pick a script--

Journal text:

**Parent description**

Script make ICMP call to Node and Returning 3 array positions: [0] Packets received (0=unreachable 1=reachable) [1] Packetloss [2] rtt

**Automation List**

Name	Result equals	Script name	Journal text
Host Reachability	==	Ping Host	Ping host
Host is up. Check Service Status	== 0:1	Check Windows Service ADV	Host is reachable, trying service script, Result [1]
Service is Disabled	== 0:2	Exit Scenario	Service is DISABLED state!!
Service Running	== 0:5	Exit Scenario	Service is running
Host Unreachable UpdateEvent	== 0:0	Update Summary and set Critical for CheckWindowsStatusADV	
Service Manual	== 0:4	Update Summary and set Warning for CheckWindowsStatusADV	
Host is down	== 0:0	Exit Scenario	The host is down. Exiting the Scenario

**Flowchart**

```
graph LR; HR[Host Reachability] --> HUS[Host is up. Check Service Status]; HUS --> SD[Service is Disabled]; HUS --> SR[Service Running]; HUS --> HUE[Host Unreachable UpdateEvent]; HUS --> SM[Service Manual]; HUS --> HD[Host is down];
```

# In action example

## Event Classification

- ObjectType
- KPI
- Service Affecting
- ShowFor
- OperationProfile
- Service
- Severity
- USD Group

- Discard
- Delay
- Escalate

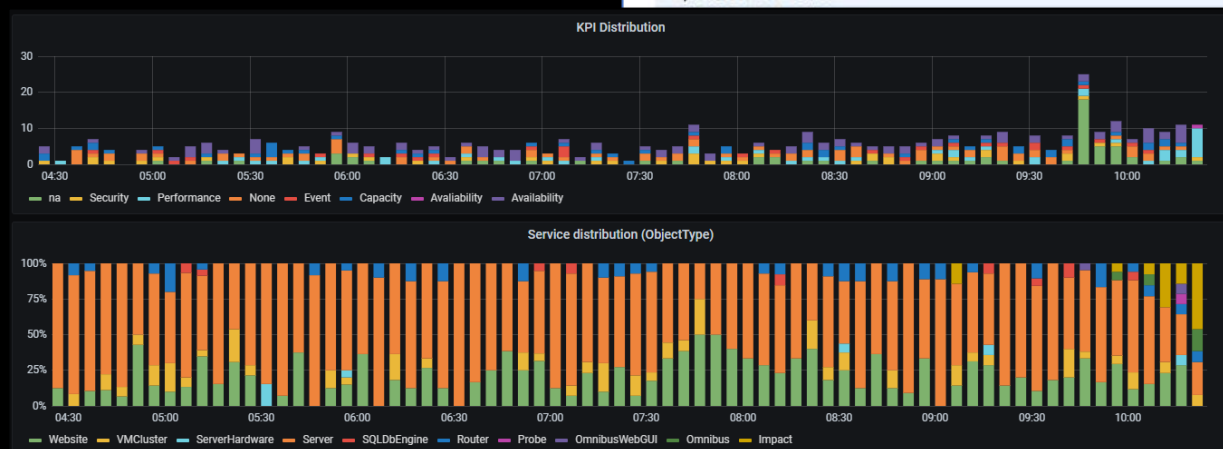
- Incident
- Mail
- SMS

- Actions

Groups  
(Customer)

## Groups per Nodes, Service, Site, ...

# Service, ObjectType

[illegible]

Event  
Classification,  
KPI, Service  
Affecting,  
SuprEscl

# Dynamic Dashboard

- Application or System centric visualization of status.
  - Application filter in dropdown
- Easy to create different dashboard for different teams.
  - Minutes per dashboard
- Realtime and historical data
- Charts, TopN-lists, ServersStatus, CI-status and eventlists
- Branding and themes
- Personal settings per user.
- Drag'n'drop layout
- Built on existing infrastructure (NOI)
- 'Any' data can be added (Impact)

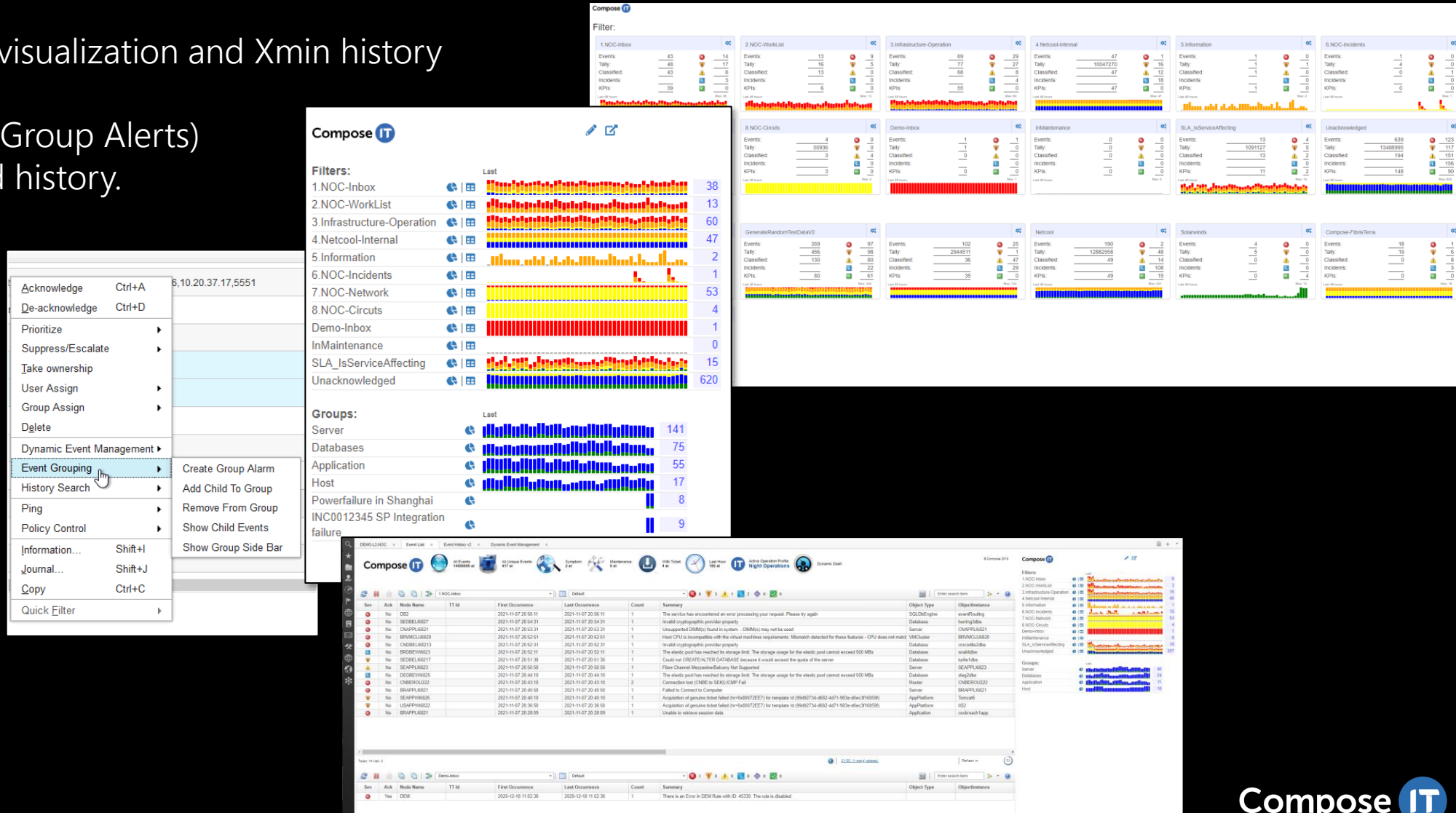




# Automatic Filter Visualization

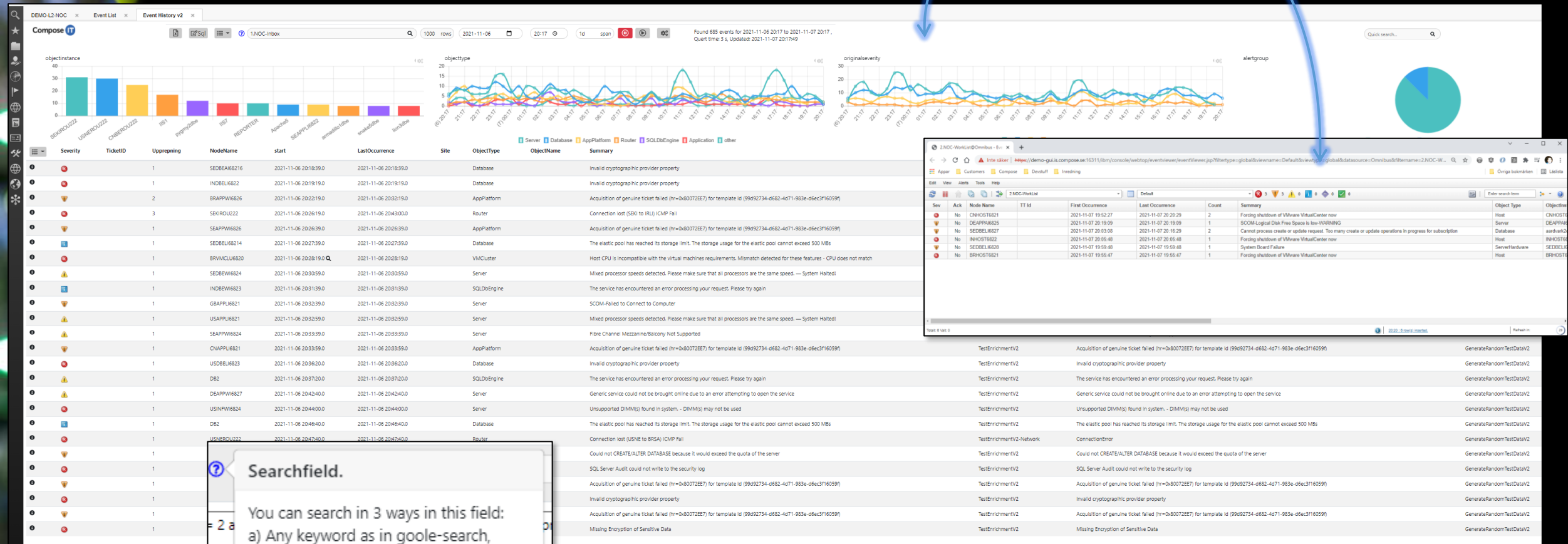
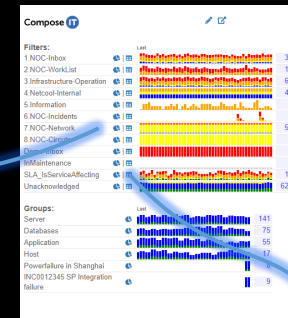
- Automatic filter visualization and Xmin history
- Dynamic 'filter' (Group Alerts) visualization and history.

- Create
- Add
- Remove
- Show
- (Detach)



# Event Statistics

Drill down to event-list  
or the event history-tool



Filter automatically available  
in history-tool

# Event Routing - DevOps logic

- Generic event classification – Dynamic Event Management (DEM)

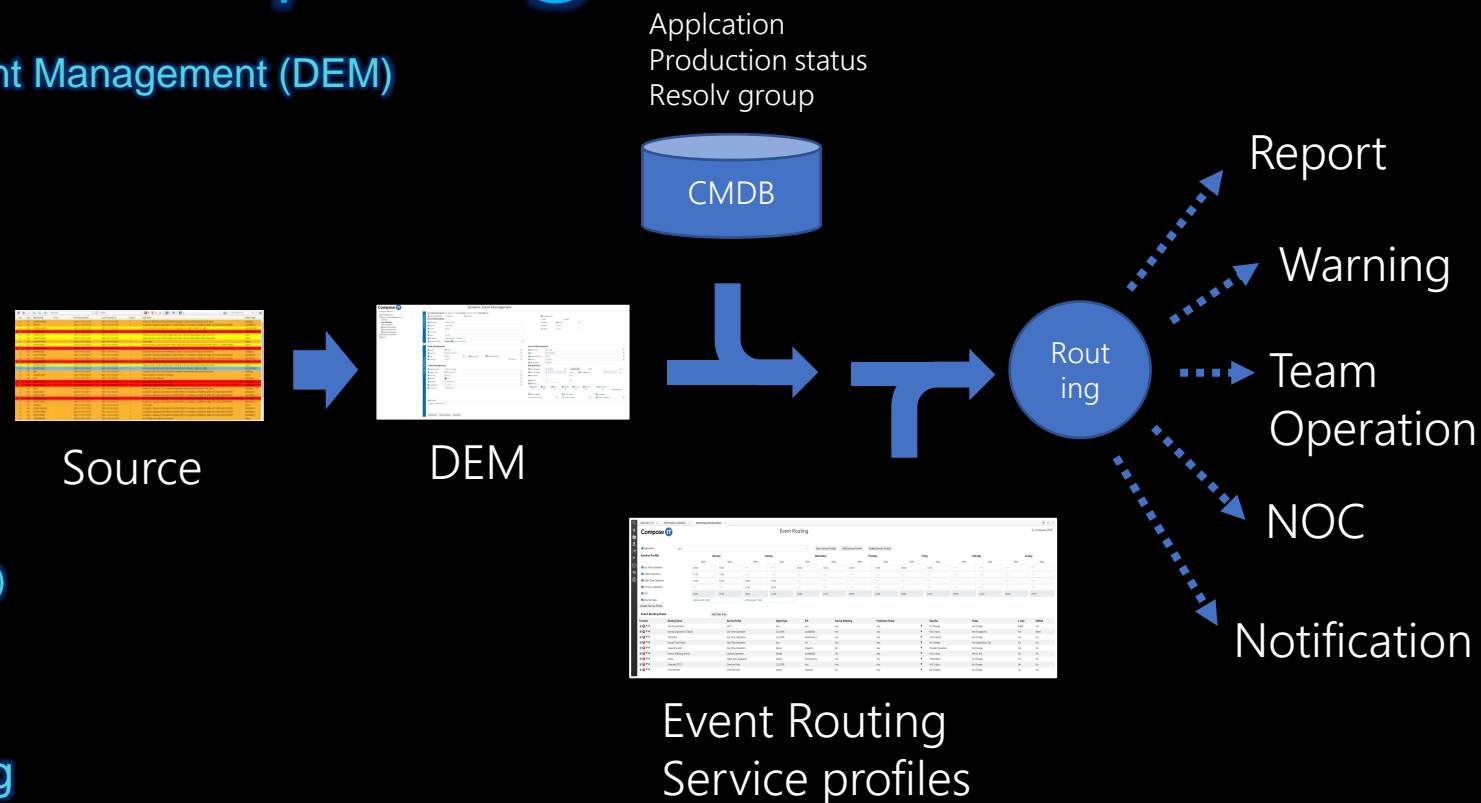
- Show For
- Object Type
- KPI
- Service Affecting
- Infra ('CI') vs Application group

- Application/Team defined – Service Profiles

- Day time Operation (full staffing)
- Limited operation (evenings ex. 17:00-24:00)
- Nighttime operation (Duty)
- Off hours (Outside service hours)

- Team + Service Profile = Event Routing

- Who to show for (Noc and/or Operational team)
- Action (notification)
- Ticket automation



# Application team/Service profiles

🔍

★

📁

👤

📅

🚧

🌐

Add Rule v.3.0

Add/Change Automation

Add/Change Routing Rules

Compose IT

Event Routing

© Compose 2018

Application

EcoAppX

View Service Profile

Add Service Profile

Delete Service Profile

Service Profile

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Start

Stop

Start

Stop

Start

Stop

Start

Stop

Start

Stop

Start

Stop

Start

Stop

Start

Stop

Day Time Operation

Limited Operation

Night Time Operation

Off Hours Operation

24/7

Override Date

Update Service Profile

Event Routing Rules

Add New Rule

Function	Routing Name	Service Profile	ObjectType	KPI	Service Affecting	Production Status	ShowFor	Ticket	e-mail	SIGNL4
🔍 ⬆️ ⬆️ ⬆️	Test Environment	24/7	Any	Any	Any	Any	➔ No Change	No Change	Reset	Yes
🔍 ⬆️ ⬆️ ⬆️	Normal Operation Criticals	Day Time Operation	CLUSTER	Availability	Yes	Any	➔ NOC Inbox	Yes (Focalpoint)	Yes	Reset
🔍 ⬆️ ⬆️ ⬆️	TESTRules	Day Time Operation	CLUSTER	Performance	Yes	Any	➔ COP Internal	No Change	No	No
🔍 ⬆️ ⬆️ ⬆️	Discard Test Events	Day Time Operation	Any	All	Any	Any	➔ No Change	Yes (Application AG)	No	No
🔍 ⬆️ ⬆️ ⬆️	Capacity Events	Day Time Operation	Server	Capacity	No	Any	➔ Domain Operation	No Change	No	No
🔍 ⬆️ ⬆️ ⬆️	Service Affecting Events	Limited Operation	Biztalk	Availability	Yes	Any	➔ NOC Inbox	Yes (CI AG)	No	No
🔍 ⬆️ ⬆️ ⬆️	Testar	Night Time Operation	Amtrix	Performance	Yes	Any	➔ Information	No Change	No	No
🔍 ⬆️ ⬆️ ⬆️	Override TEST 2	Override Date	CLUSTER	Any	Any	Any	➔ NOC Inbox	No Change	No	No
🔍 ⬆️ ⬆️ ⬆️	Override test	Override Date	Amtrix	Capacity	No	Any	➔ No Change	No Change	No	No



🔍

★

📁

👤

📍

🚩

📡

🔧

🌐

Add Rule v.3.0 ×

Add/Change Automation ×

Add/Change Routing Rules ×

Compose IT

Event Routing

Application:

EcoAppX

📘 Routing Name:

Capacity Events

📘 Service Profile:

Day Time Operation

Incoming routing rule

📘 ObjectType:

Server

📘 KPI:

Capacity

📘 Service Affecting:

No

📘 Production Status:

Any

↓

Outgoing routing rule

📘 ShowFor:

Domain Operation

📘 Ticket:

Yes (Application AG)

📘 e-mail:

No e-mail

📘 SIGNAL4:

EcoX Beredskap

📘 Comment:








Update Rule

Back

Compose IT

# Result



- Ever changing environments  ✓ Fast adoption of new events sources by Event Classification
- Different demands from different consumers  ✓ Granular rules to manage events and outcome
- Changing operational model  ✓ Datamodel let you make changes to logic without having to rewrite filters, reports and dashboards
- Correct operational information  ✓ Powerful classification and management of events and logic, fast to deploy custom dashboards
- TTM (Time to market)  ✓ Flexible model and easy to adopt to new needs
- Different OLA/SLAs  ✓ Granular model and meta data compatible
- Less resources  ✓ Do more, faster, no technical specialists necessary

# Compose IT can support your journey

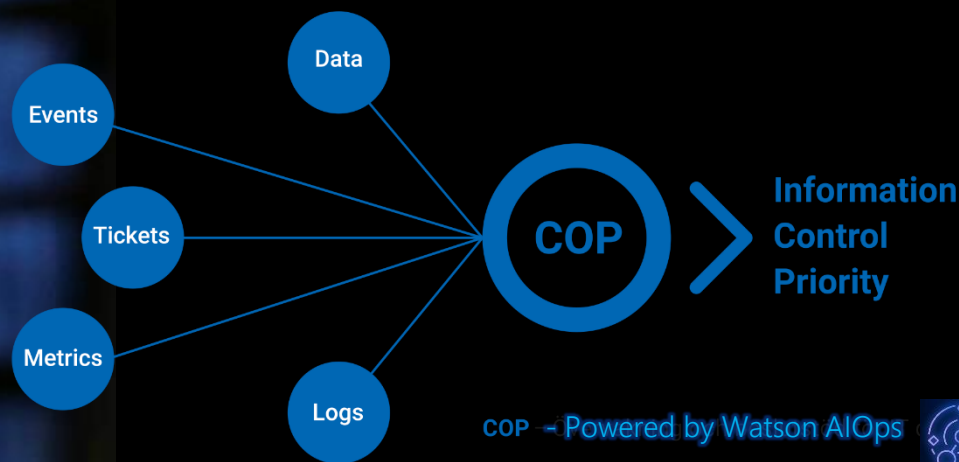
[www.compose.se](http://www.compose.se)



## Central Operation Platform

A 'turnkey ready' adaption of Watson AIOps and Elastic with more than 600.000 hours of experience built into both the tools and the way of working.

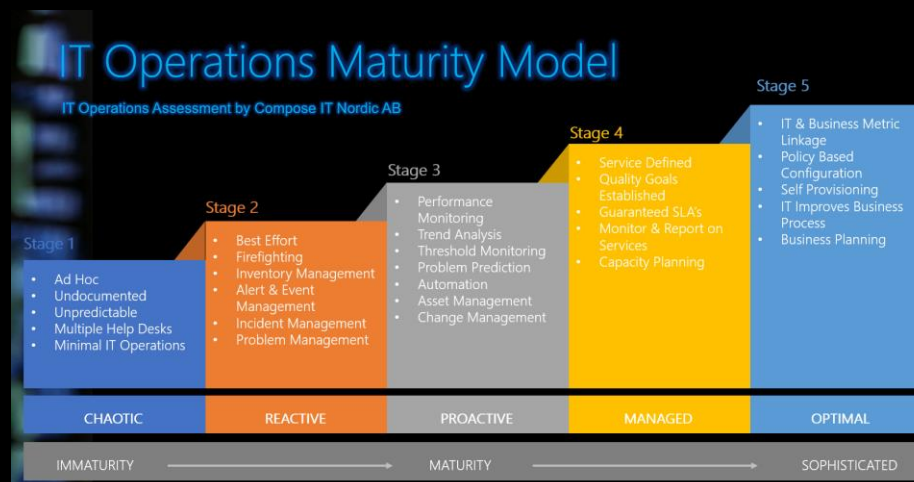
For new or existing users of Netcool/Watson AIOps



## Where are you and what's your next step?

IT Operation Assessment Service, by Compose IT

- Identify where you should put your effort to take the next step to a mature IT operation environment.



Thank you,  
questions?