ZABBIX SUMMIT ONLINE /2020

SECADM SECURE FOR SURE

# Managing complexity in Zabbix installations with Splunk

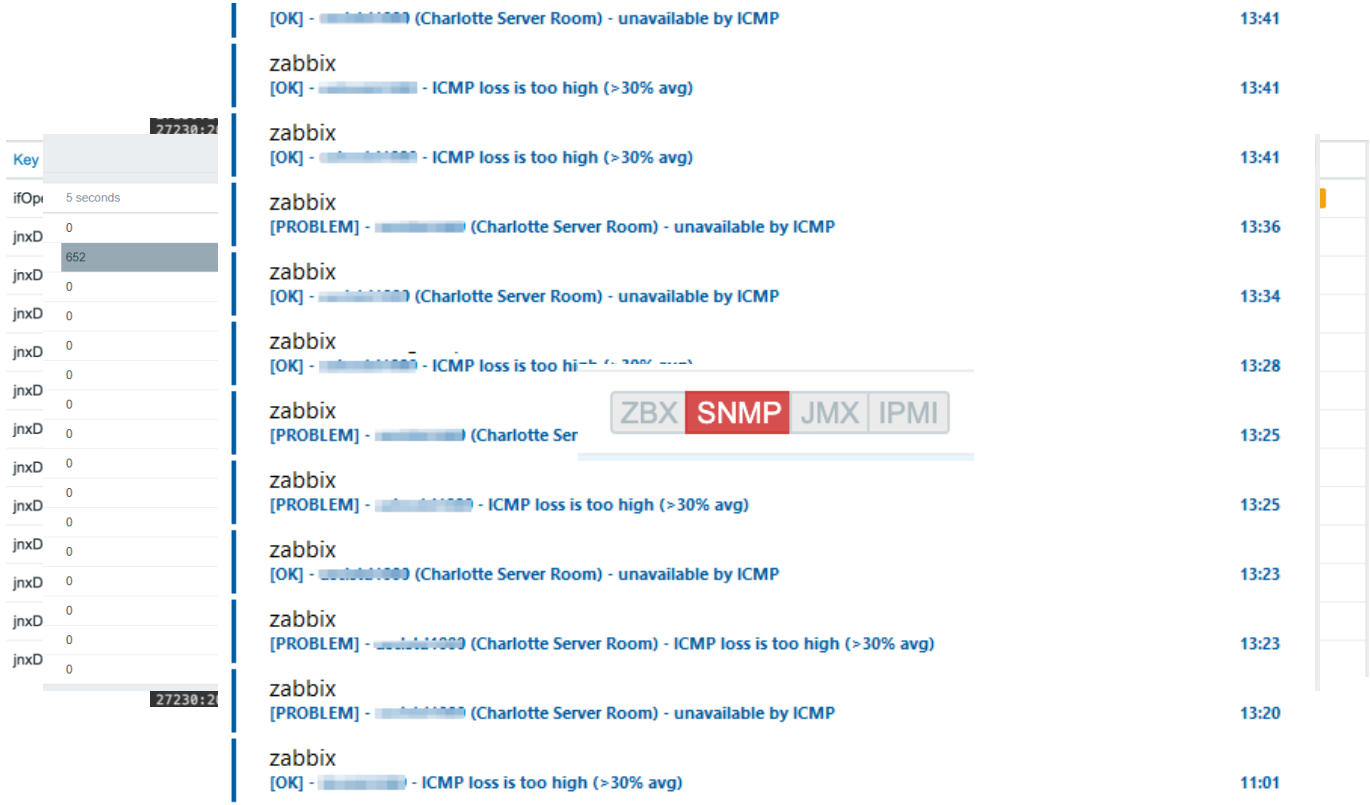
Christian.Anton@secadm.de

SECADM SECURE FOR SURE

# What complexity?

Operating a Zabbix deployment of a certain size comes with some challenges.

- Huge amount of **Hosts**, Templates, **Items**, Host Groups, Macros, …
- **Unsupported** Items / LLD rules
- **Network** issues / Host **availability**
- **Queue** entries
- Many many **problems**




# Questions

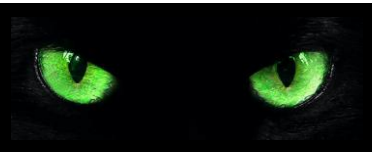
*What are the hosts generating most of the problems, at what times and generated by which templates?*

*Did the latest change / upgrade / … have any negative impact on our monitoring?*

*Can you work on getting rid of those unsupported items?*

*How many hosts we have that have this specific problem and would be the effect if we fixed those problems?*

*Where the *** do all these queue entries come from?*



# Too much information?

## Zabbix is:

- A brilliant monitoring tool
- Great ways to organize entities with templates
- Very clear and predictable
- Great visualization capabilities

## Zabbix is NOT:

- An analytics utility
- …offering a flexible query language
- …having on-demand statistical functions
- …allowing us to enrich data with arbitrary sources

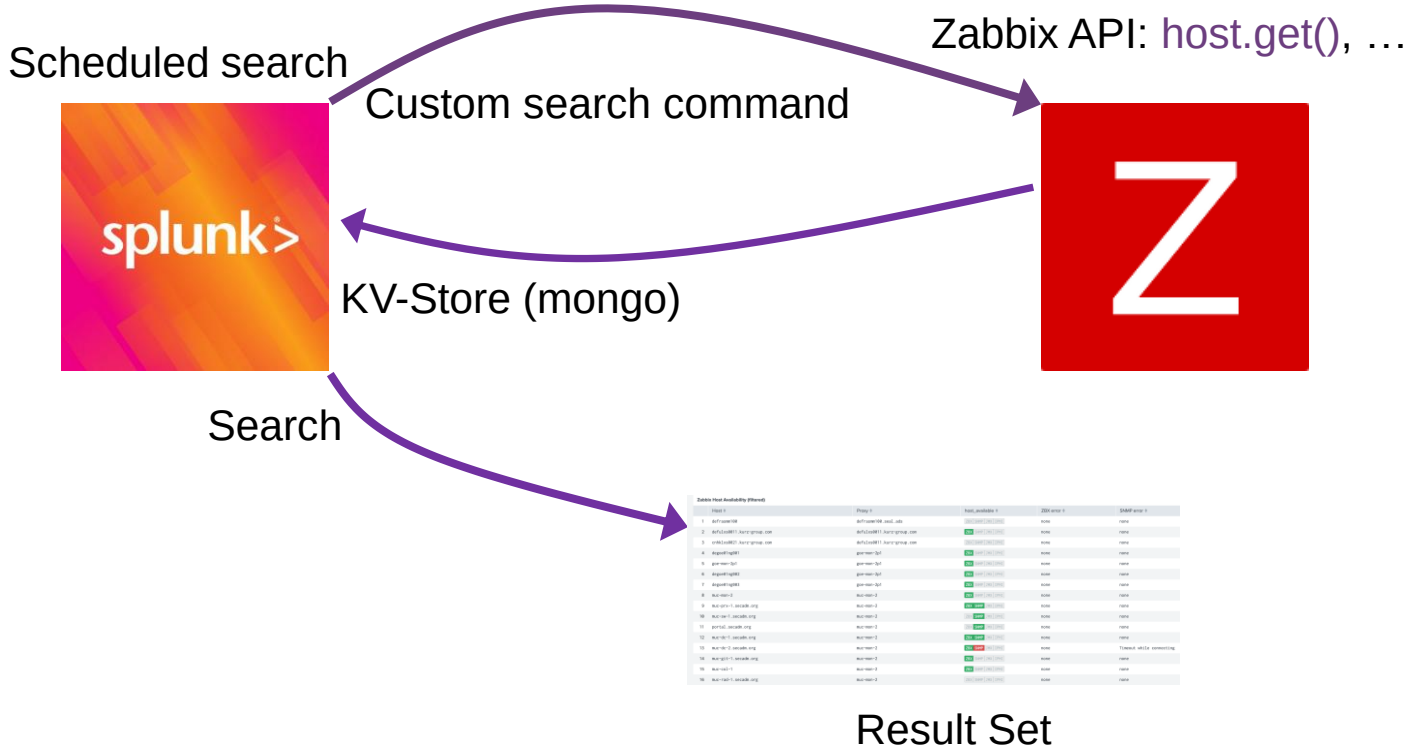
SECADM
SECURE FOR SURE

# Analyze Zabbix data with Splunk


- Data Sources depending on use case
  - Indexed data
  - Lookups backed by Key-Value store
  - Scripted lookups
  - Custom Search commands

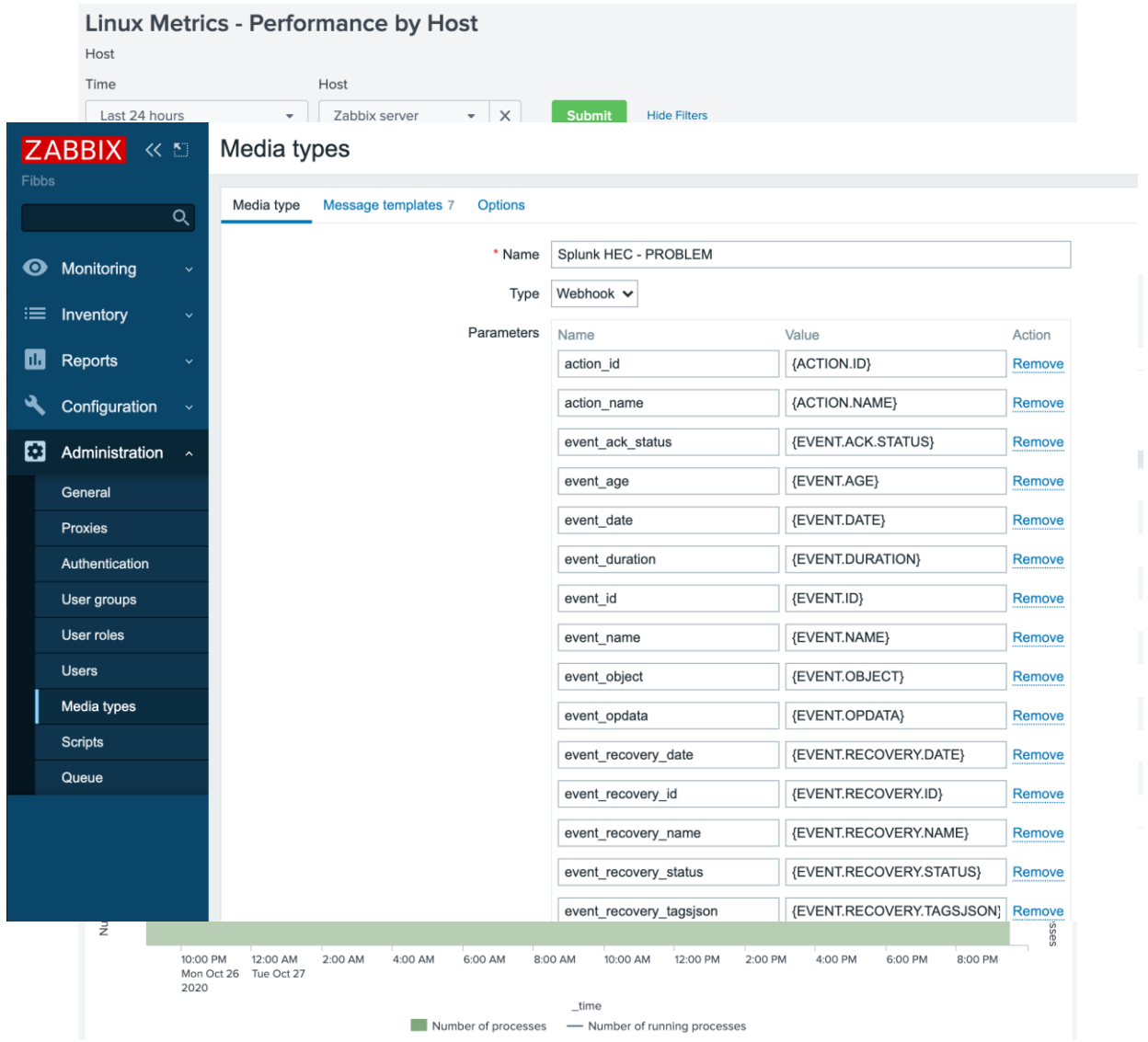
# Zabbix entity inventory

- Hosts
- Items
- Proxies
- Templates
- Triggers
- Discovery Rules (LLD)
- Item Prototypes
- Trigger Prototypes



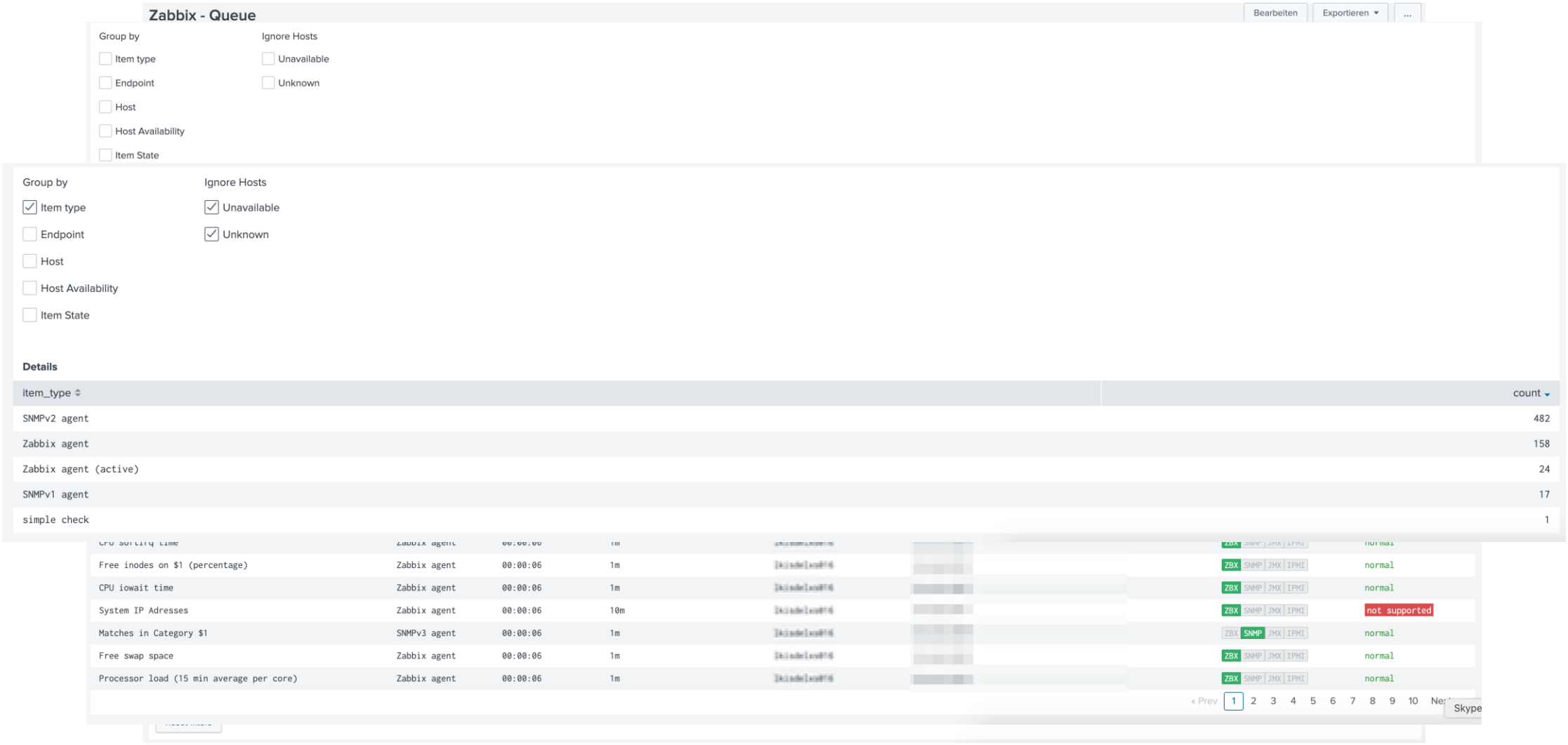
# More data

- Zabbix Server / Proxy Logs
- Real-Time lookup for status (item, host, trigger)
- Metrics (History / Trends data)
- Problems (custom Media Type)
- Alerts
- Queue items
-

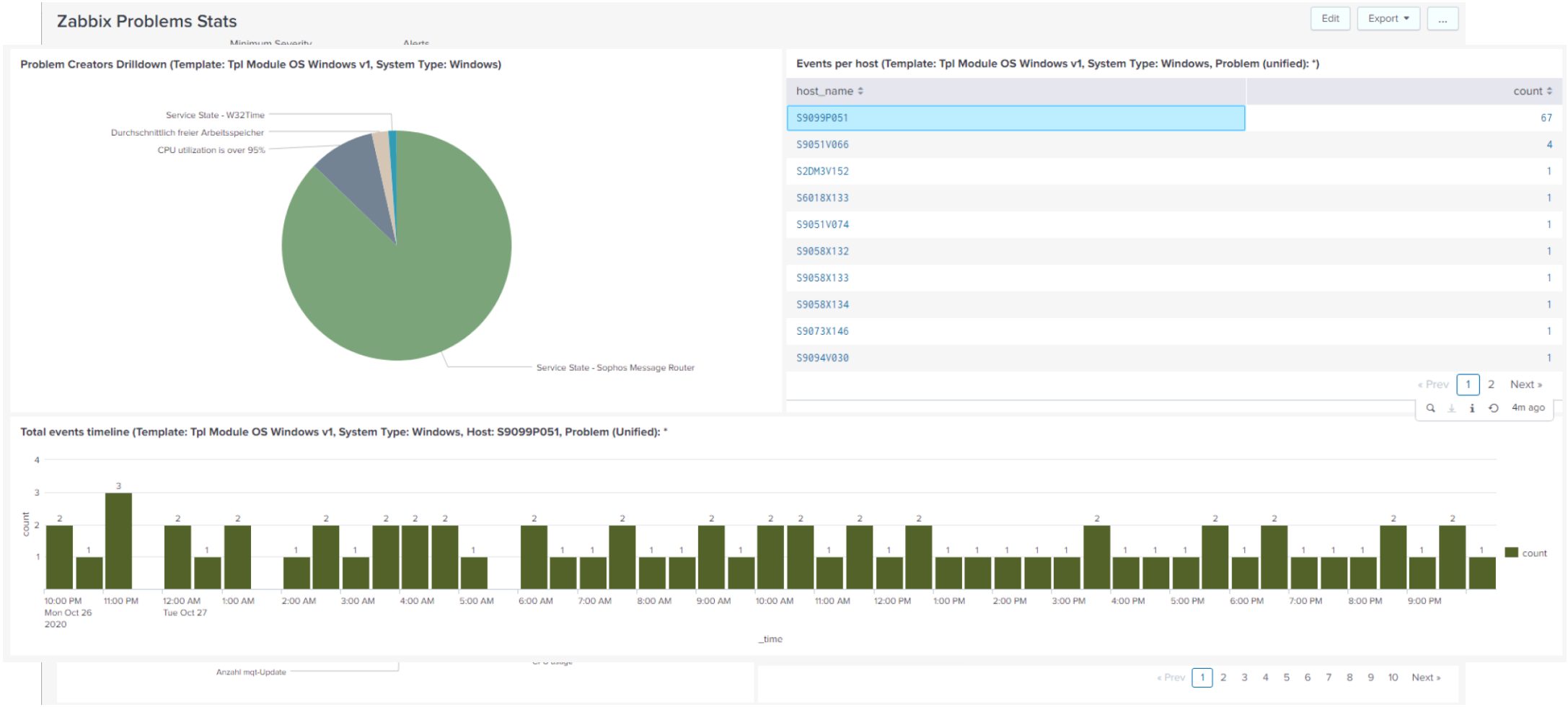


SECADM
SECURE FOR SURE

# The Zabbix Queue

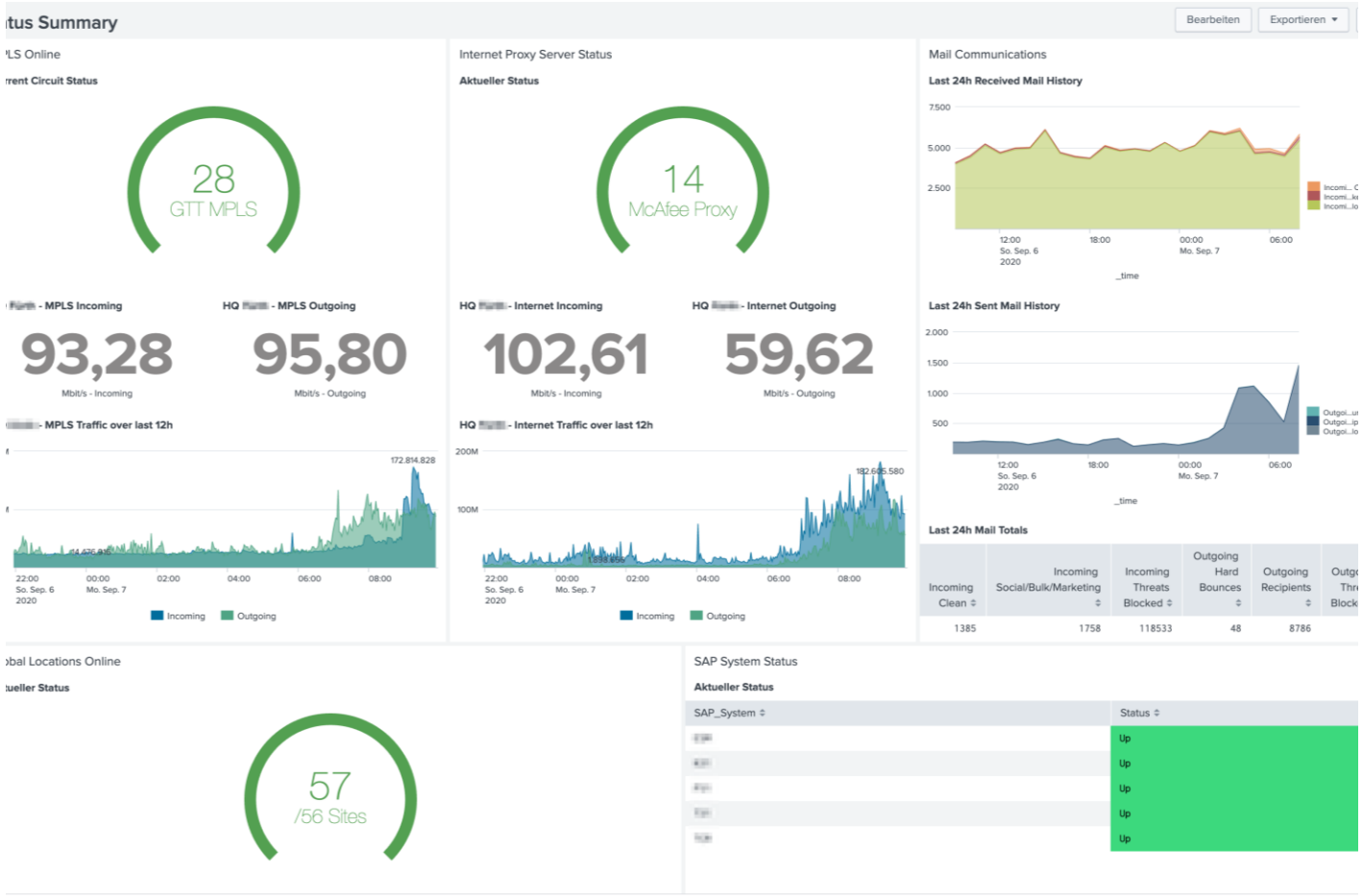


# Zabbix Problem Analytics




SECADM
SECURE FOR SURE

# Zabbix data for Management Visibility




- Correlation of data
  - Zabbix (Metrics, Status, Problems …)
  - Application Logs
  - Other data sources
  - Inventory (CMDB, …)
- Business Level Visualization

# How to get it?

- Open Source License
- Free

# Contact us!

Christian.Anton@secadm.de


SECADM
SECURE FOR SURE