Monitoring a National Power Grid With Splunk and ITSI

Linus Myrefelt, Statnett Splunk Ninja

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

No Photos

This deck contains proprietary information, no photos or video recording please!

Agenda

1. Introduction
2. Monitoring the National Power Grid Using Splunk
3. IoT in the OT World
4. The Road to Splunk ITSI
5. Lessons Learned

LINUS MYREFELT

Statnett Splunk Ninja

MY BETTER SELF

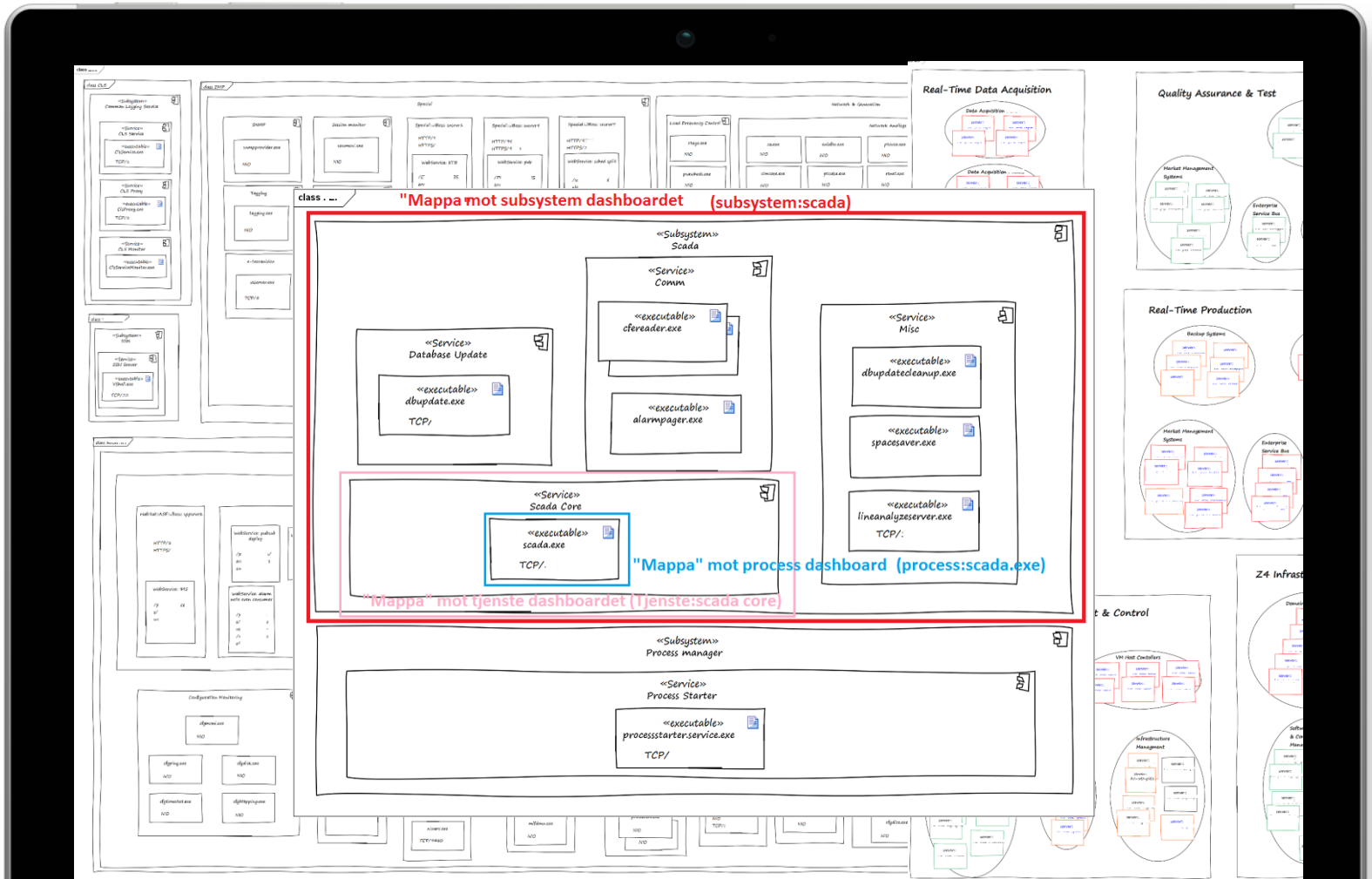
My Mini Me


Statnett

What is EMS?

- EMS
  - Also a term SCADA/EMS is used) supervises, controls, optimizes, and manages generation and transmission systems
  - EMS enables utilities to collect, store, and analyze data from hundreds of thousands of data points in national or regional power systems, perform system modeling, simulate power operation, pinpoint faults, preempt outages, and participate in energy trading markets

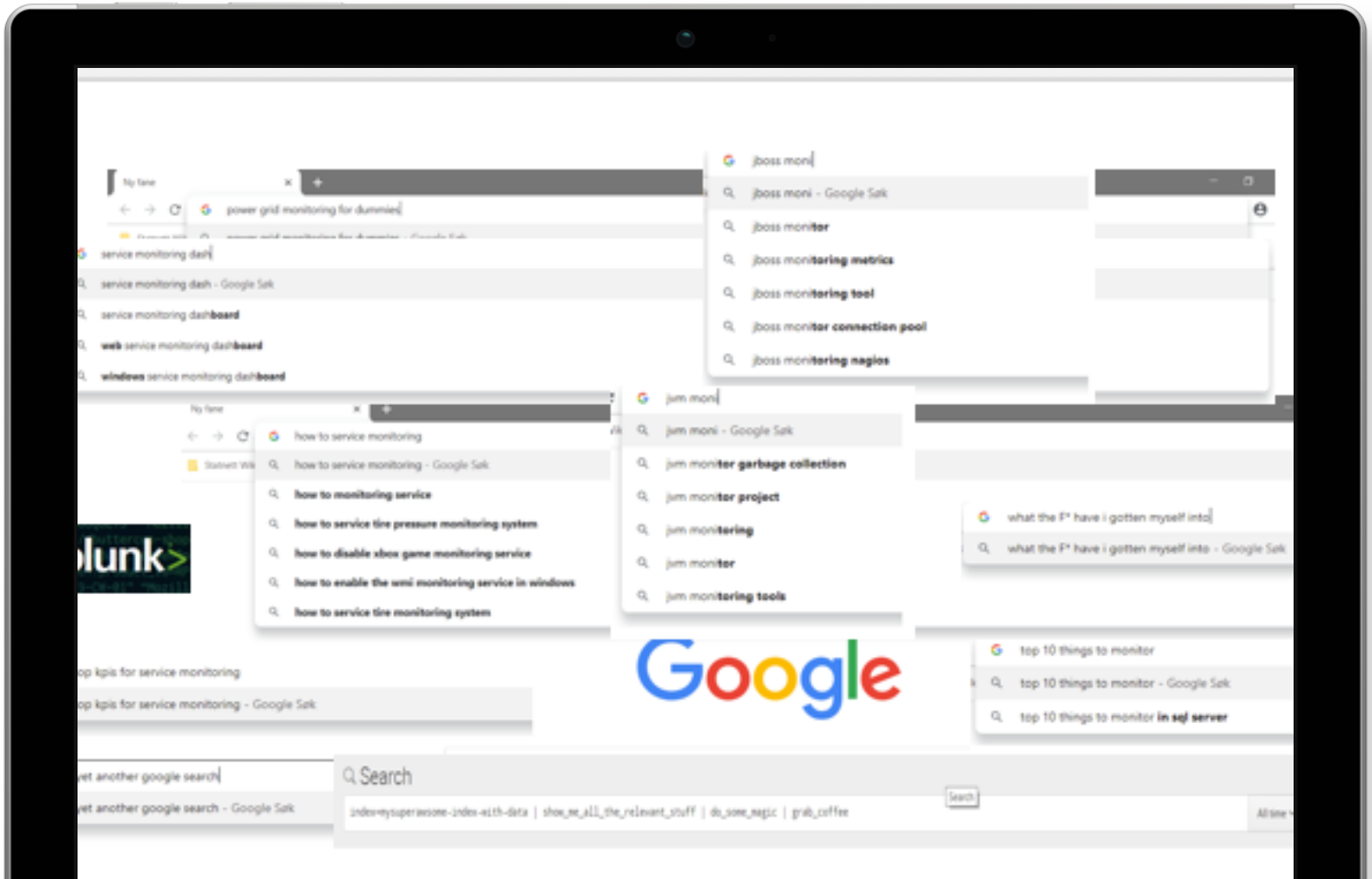
Input and Data Sources



- Inputs
- System diagram
- Plattform diagram
- Network / service architeture diagram
- Excel sheet with important processes / message codes / "metadata»
- Screenshots

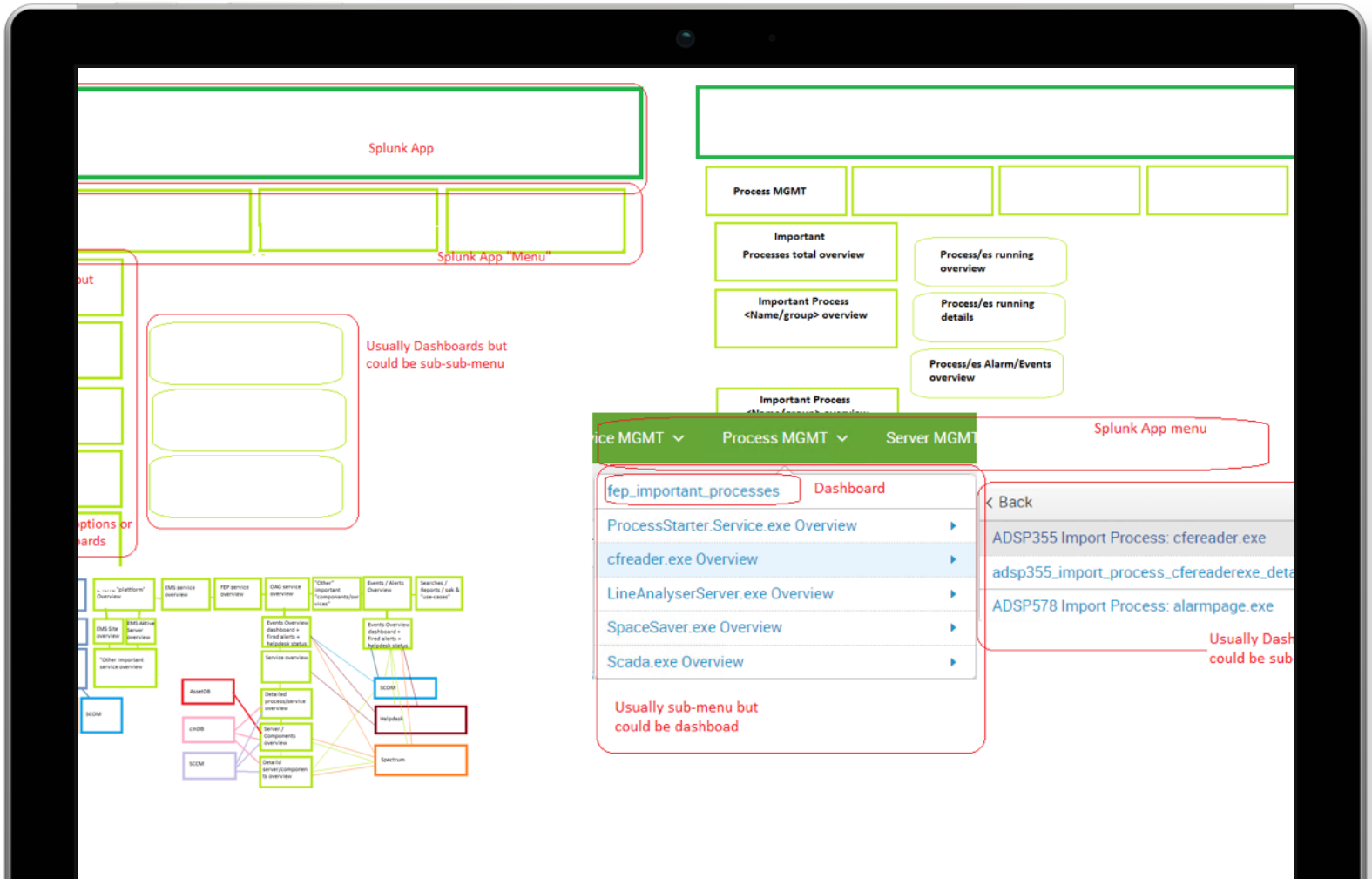
splunk> .conf18

Research Phase



- Define what a service is and its various states
- Define requirement for monitoring
  - Utilization
  - Server Monitoring
  - Can we correlate this?
  - Other monitoring tools?

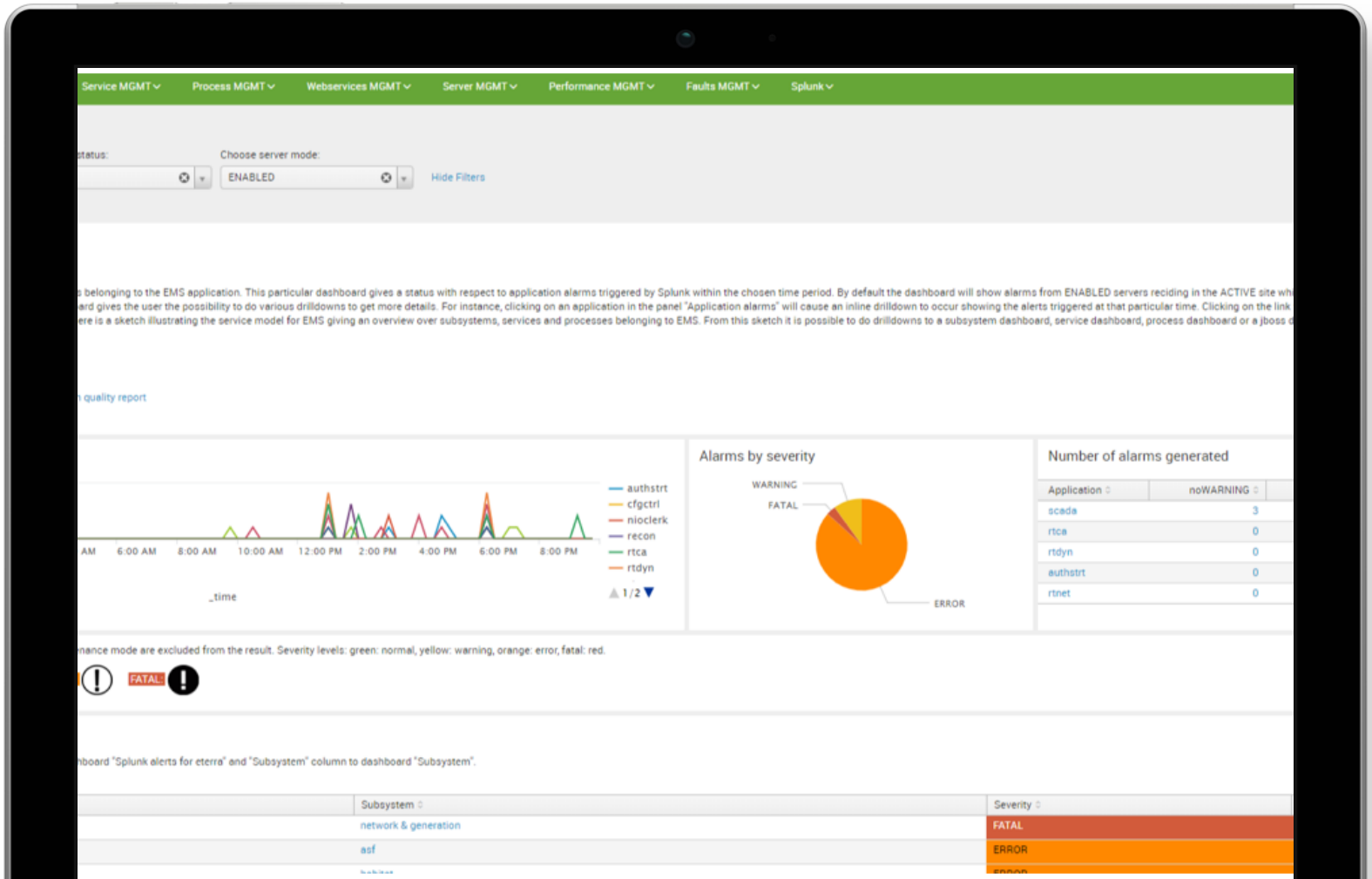
Developing Splunk Apps



- Create mockups before
- We created a handful of “apps” separated by role and function
- We wanted a high level subsystem view and detailed service view

splunk> .conf18

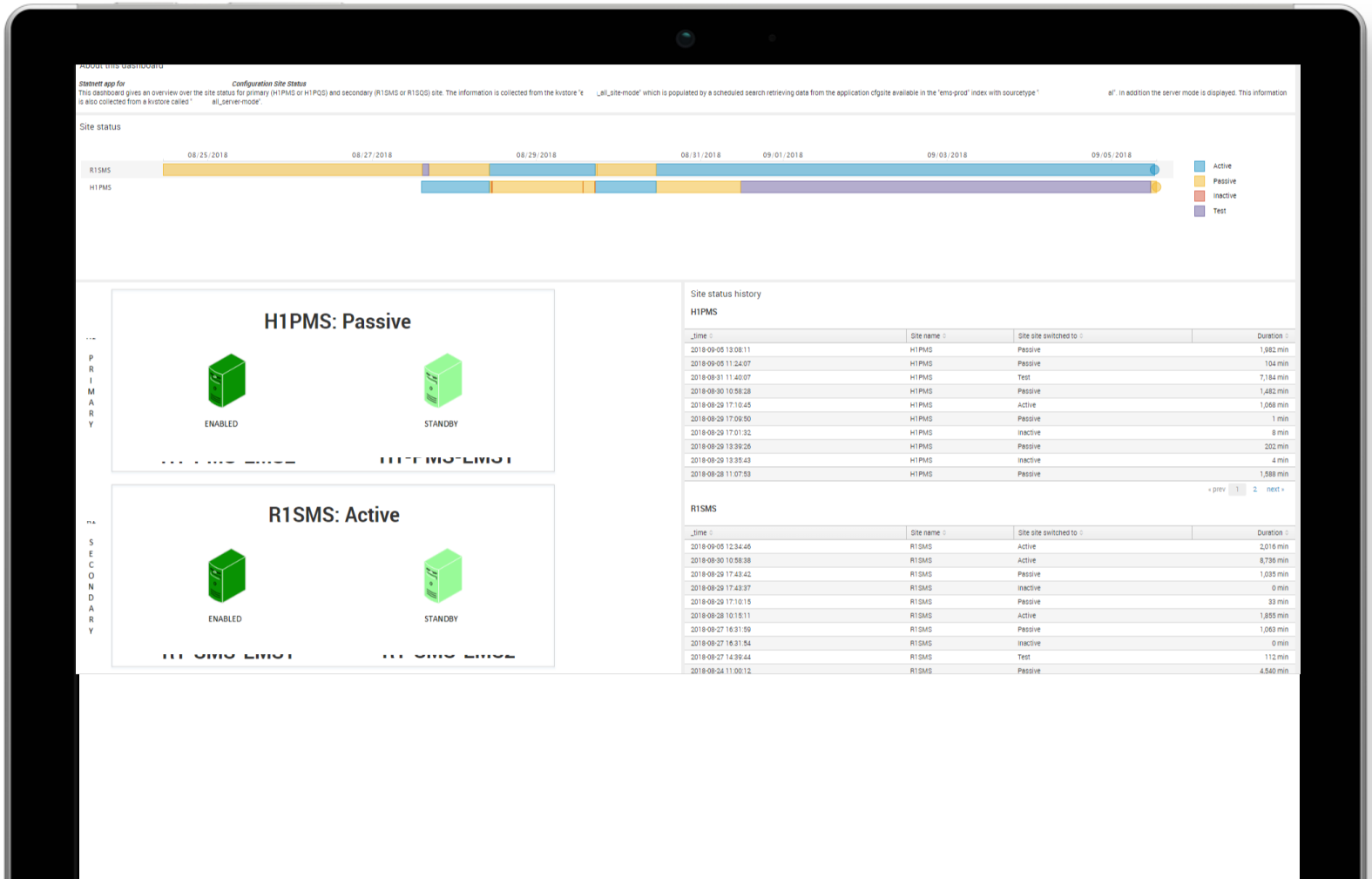
The Results



- This is the start page of each Splunk App
- Contain the most necessary information
- While also enables you to drill down into the details and alerts
- Bridges together the IT/OT environments

splunk> .conf18

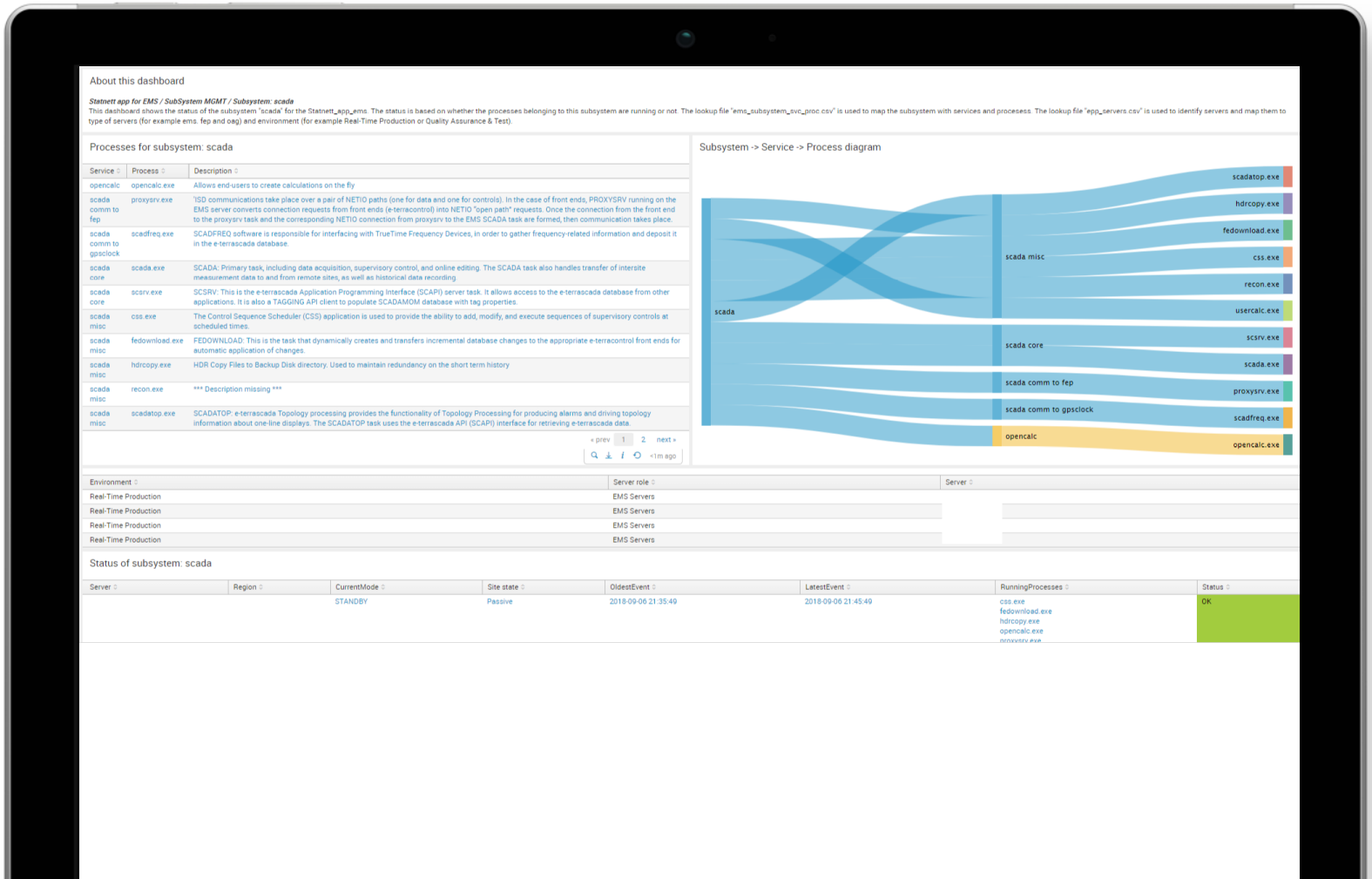
The Results



- Contain info and stats around node and site failure with the EMS
- State of system helps to dictate urgency
- Use lots of lookups and KV Collections to monitor the state

splunk> .conf18

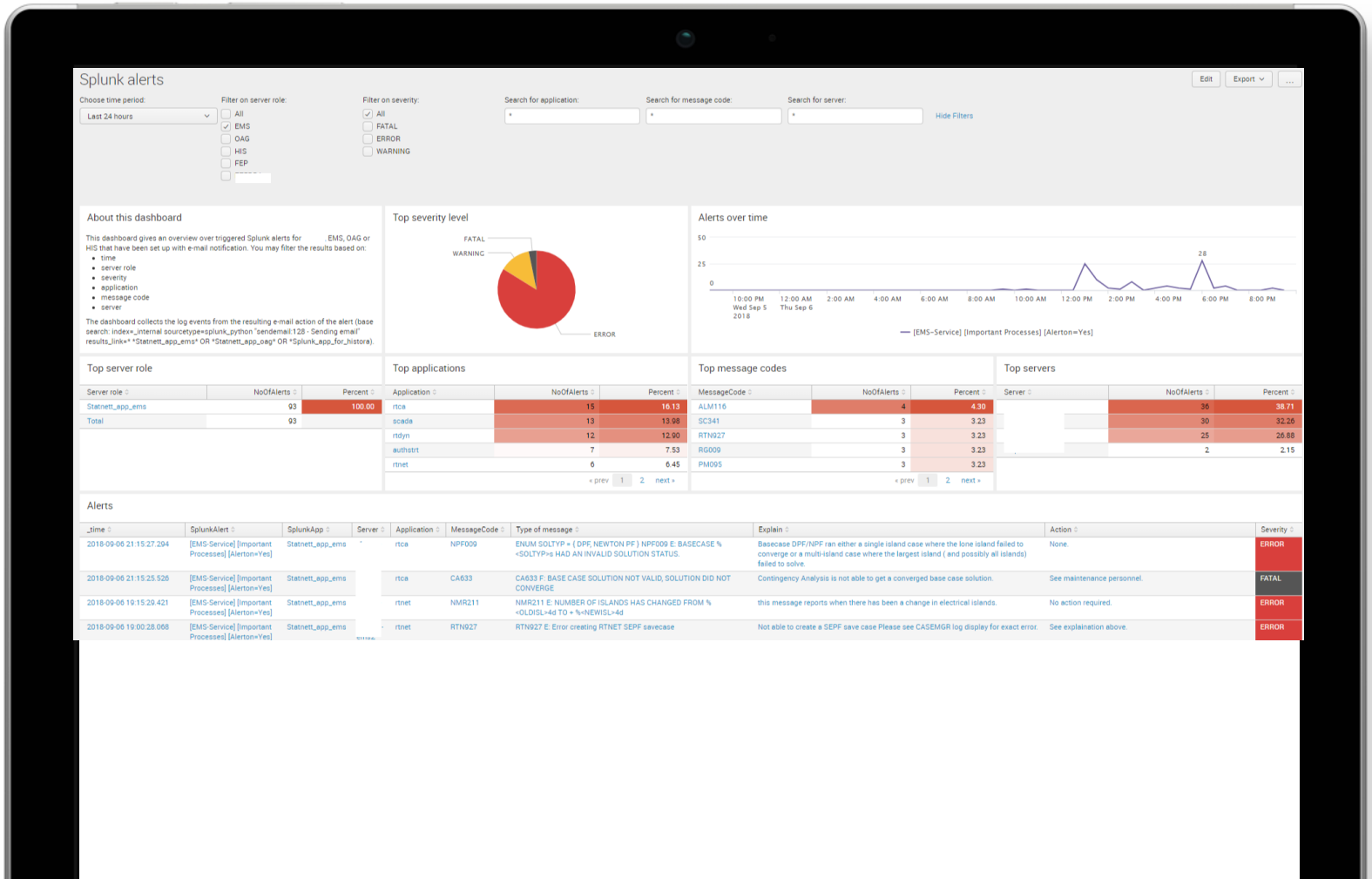
The Results



- Subservice dashboard contains description
- Higher level information is a "defined" subsystem

splunk> .conf18

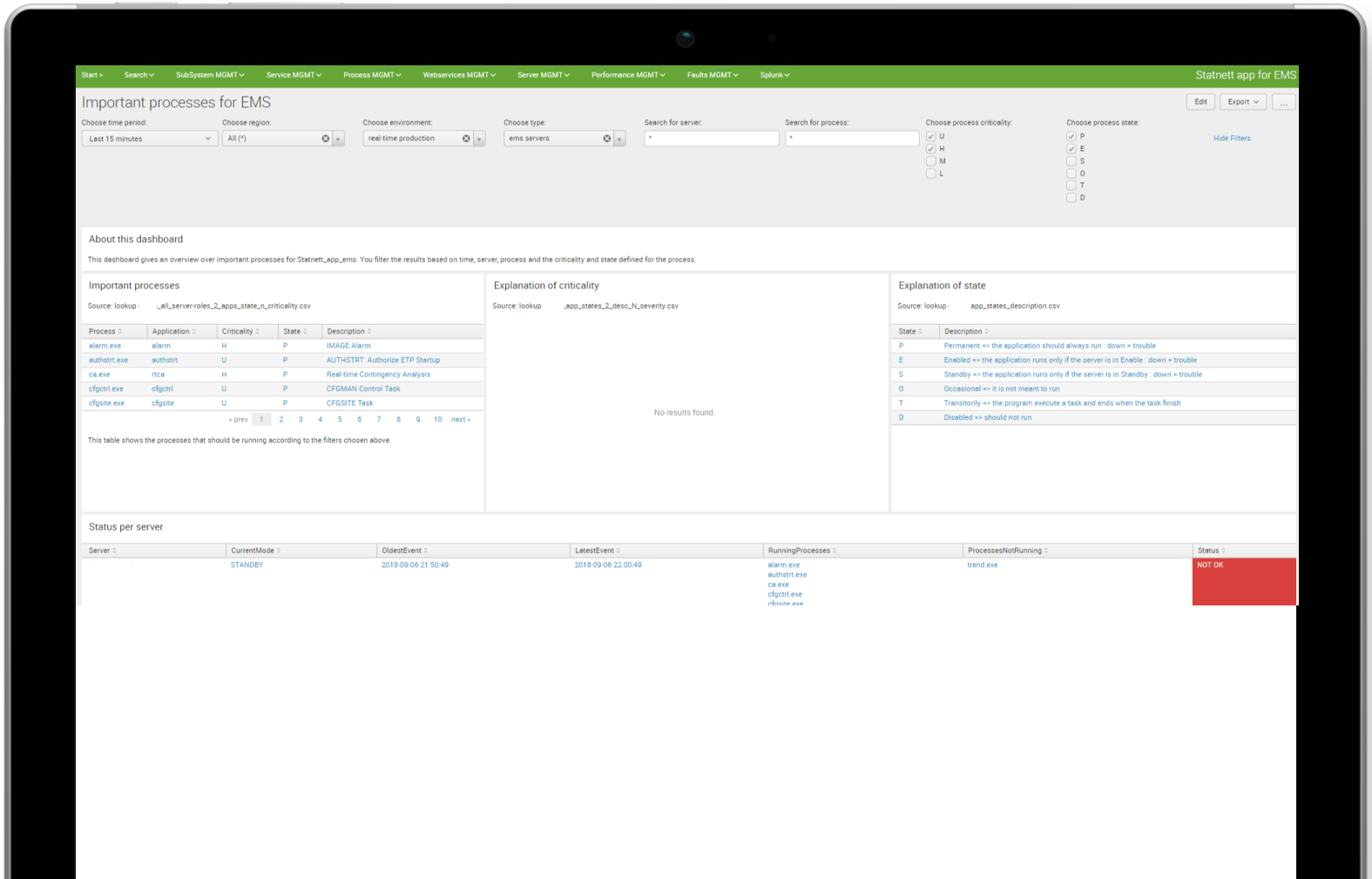
The Results



- Centralized overview of alerts generated from Splunk

splunk> .conf18

Application and Process-Focused Dashboard



- Centralized overview of Processes

splunk> .conf18

Sample Report

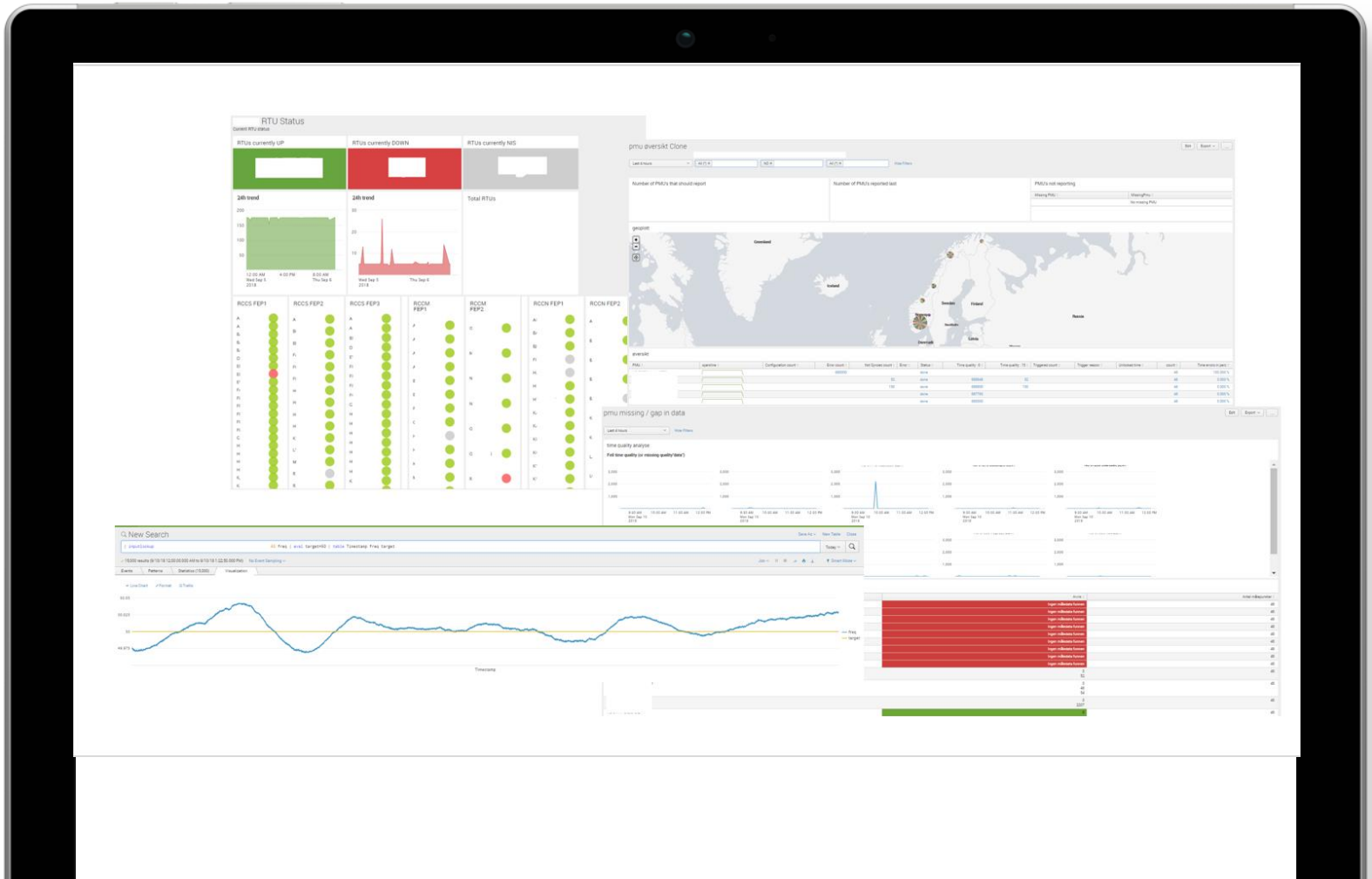
- Example of report generated based on collected scada data

splunk> .conf18

IoT in the OT World

- RTU: Remote terminal unit
  - Collects and transfers data
  - Responds to and executes commands and order the EMS
- PMU: Phasor measurement unit
  - A device which measures the electrical waves on an electricity grid using a common time source

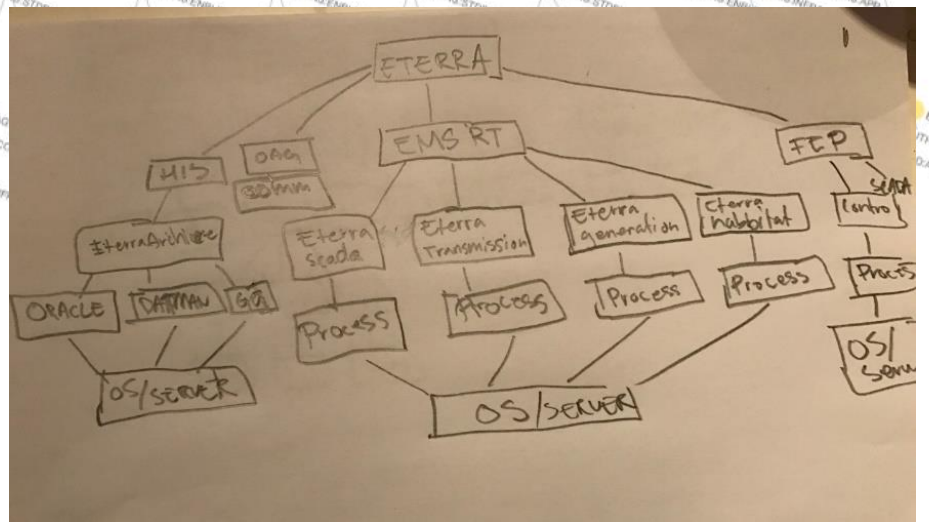
IoT Dashboard

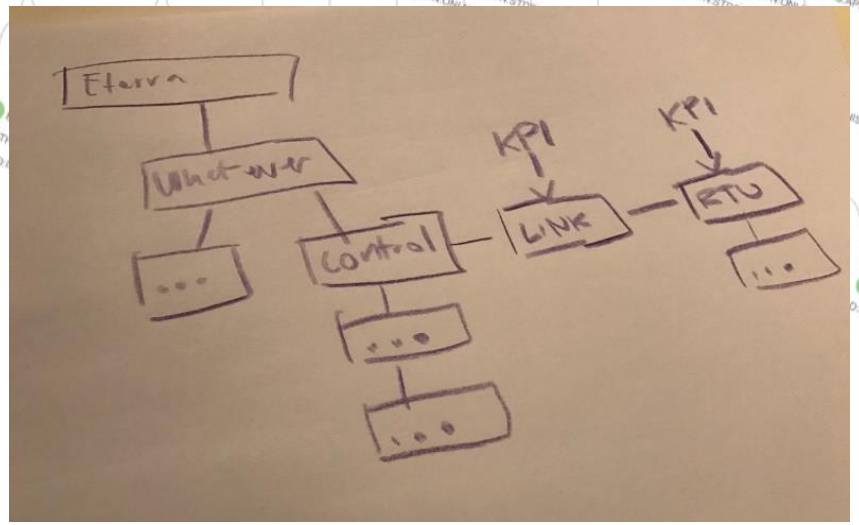


- Yey, we do IoT stuff

The Road to ITSI Enlightenment

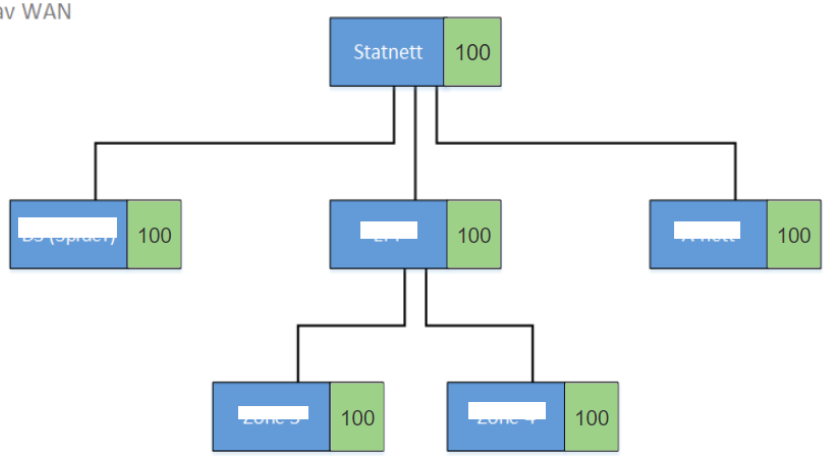
ITSI Mock-ups

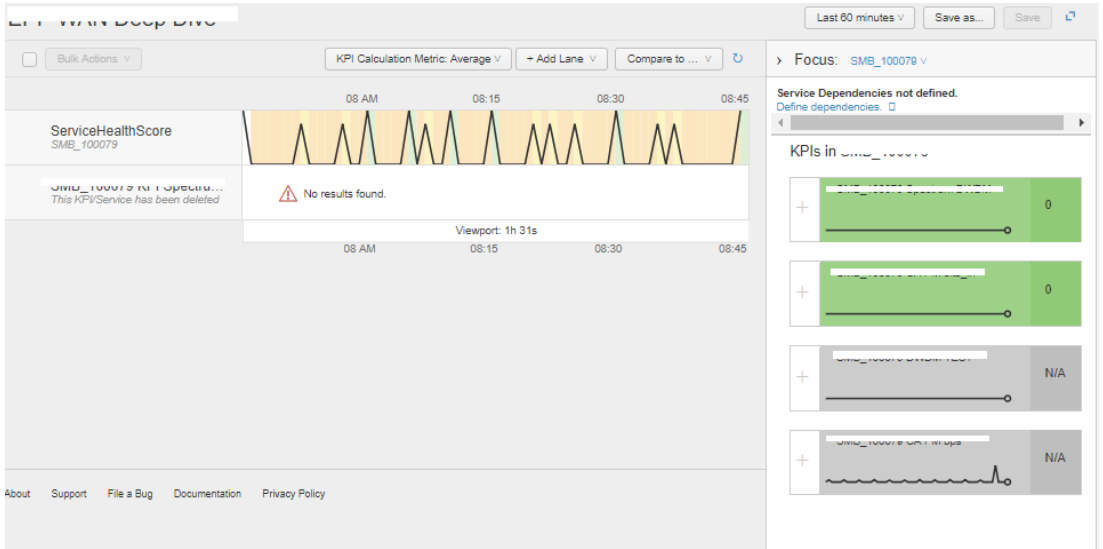


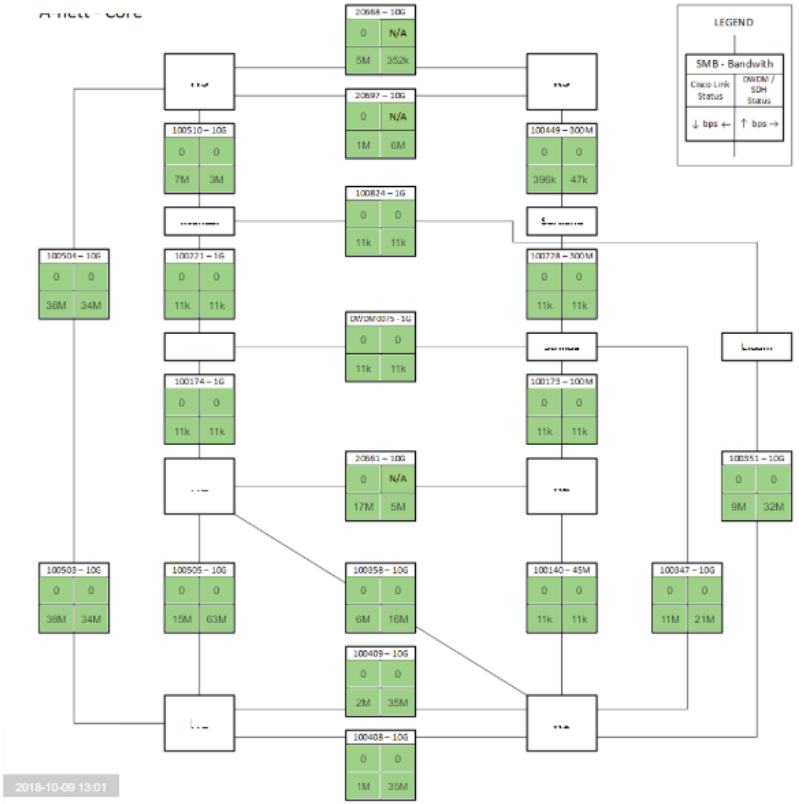


Infrastructure Glass Table Examples

Statnett
Overvåking av WAN

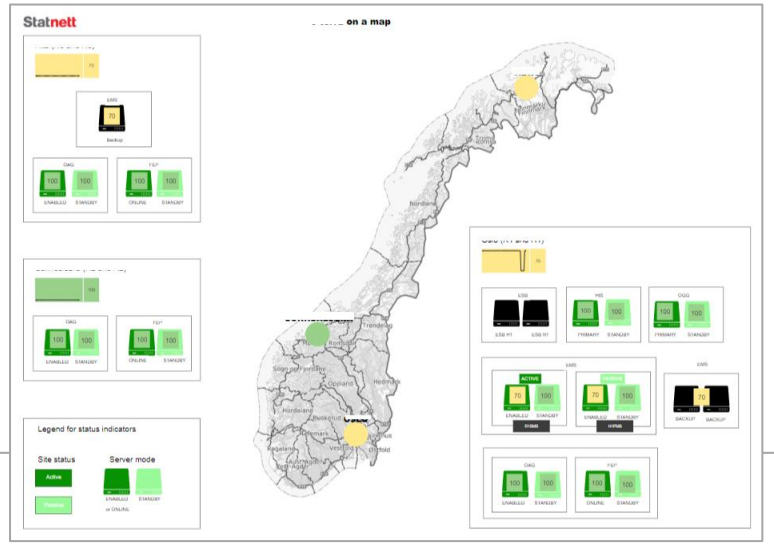


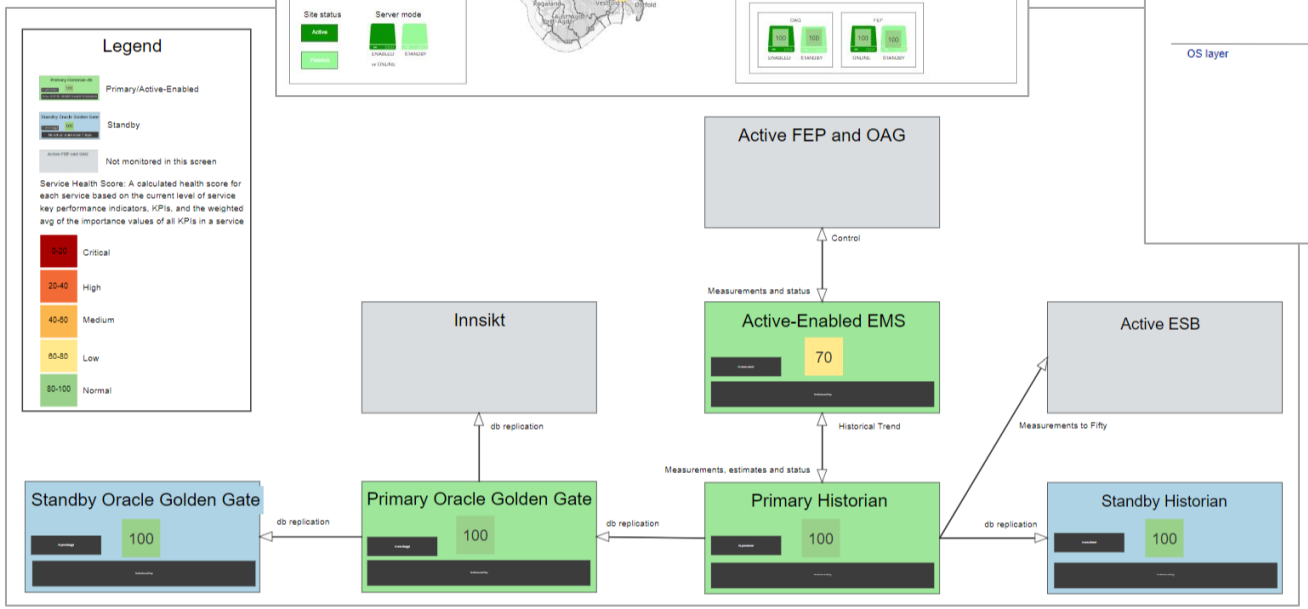




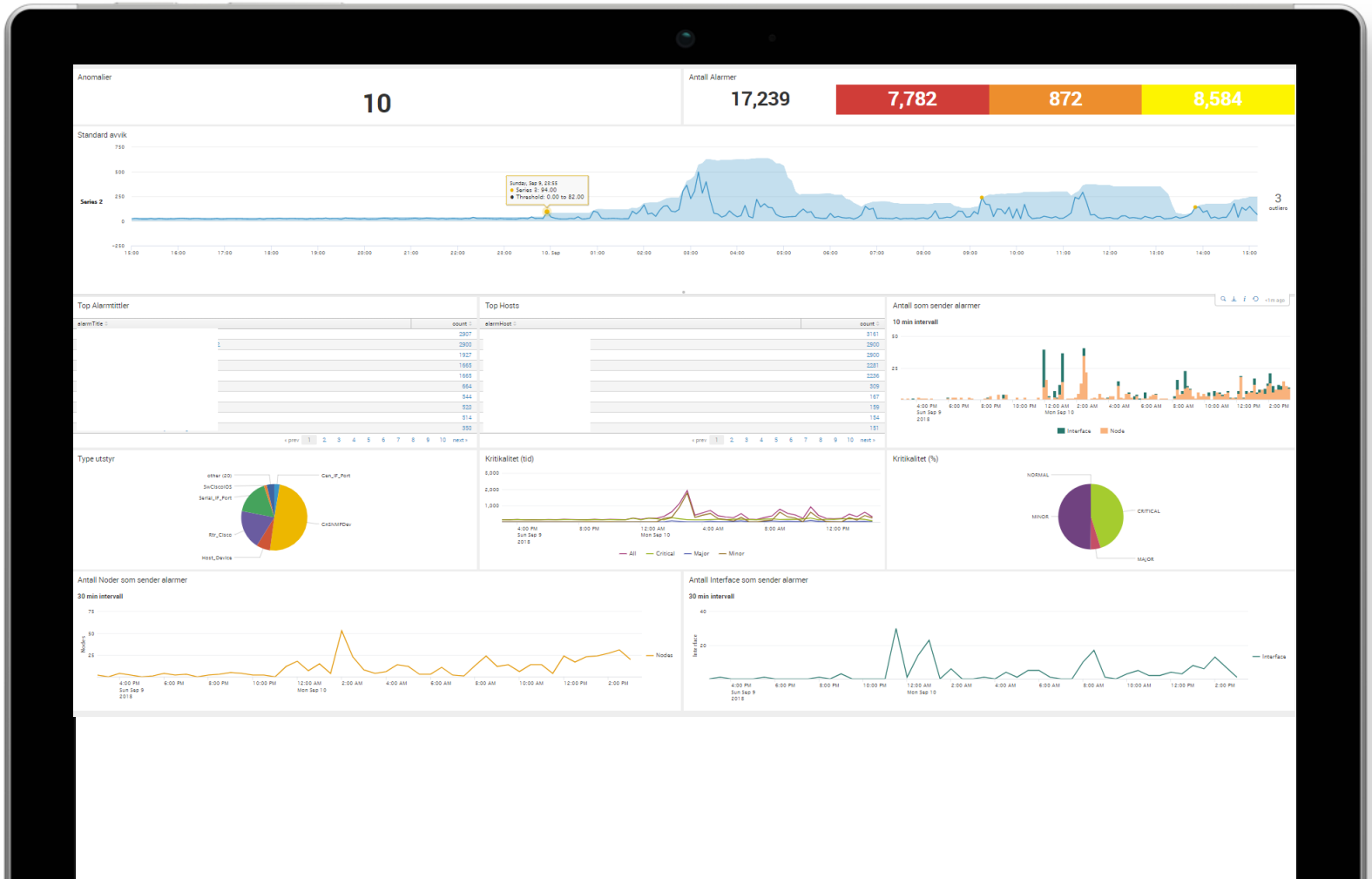
splunk> .conf18

Scada Focused Glass Tables





Machine Learning and Lessons Learned



- Playing around with Machine Learning

splunk> .conf18

Lessons Learned

Thank You!

Don't forget to rate this session in the .conf18 mobile app