Diplomarbeitspräsentation

Classification and Monitoring of Incidents in Cloud-based Big Data Analytics

Manfred Halper

Technische Universität Wien
Institute of Information Systems Engineering
Distributed Systems Group
Betreuer: Privatdoz. Dr.techn. Hong-Linh Truong

Masterstudium:
Software Engineering/Internet Computing

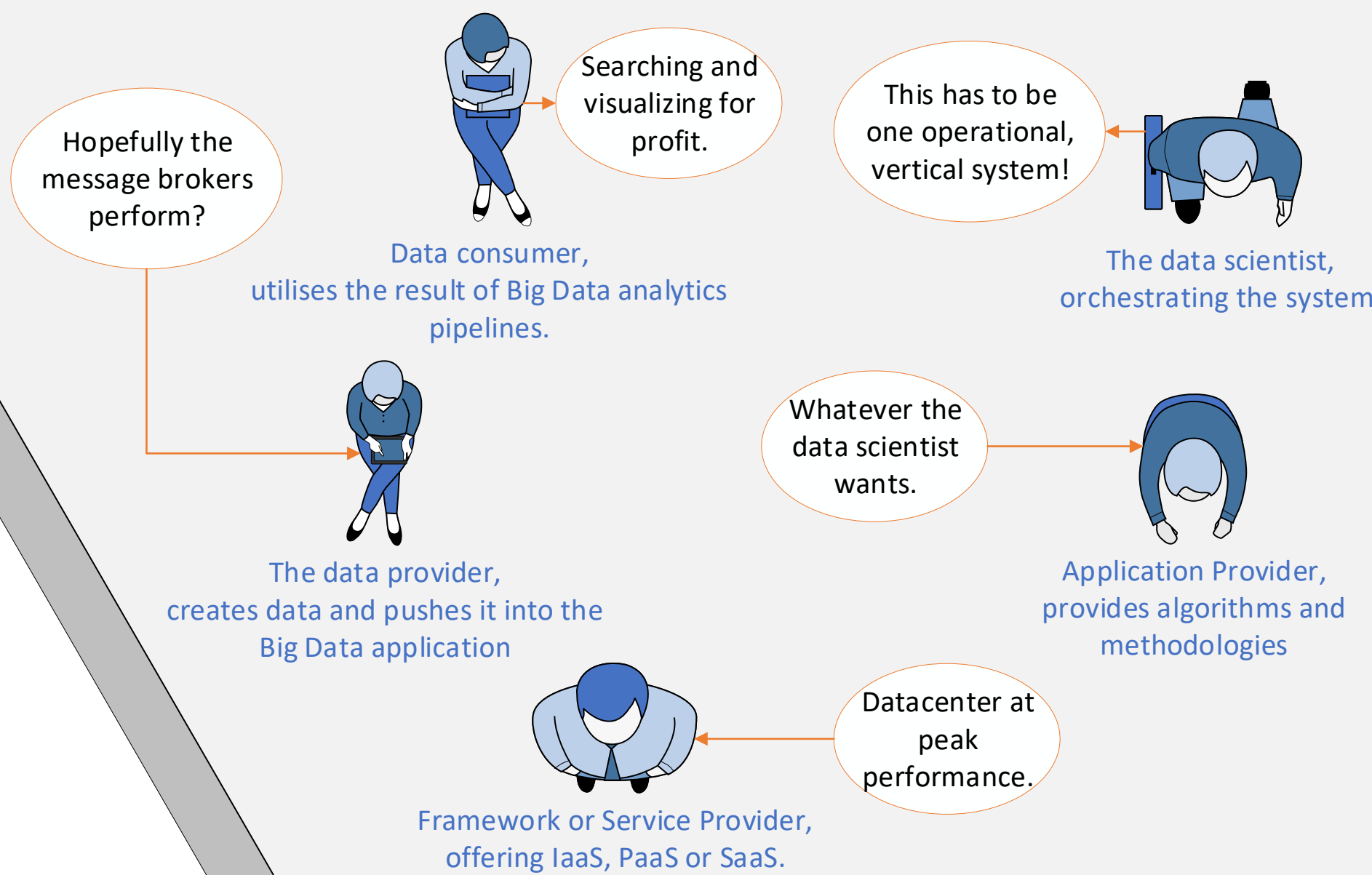DISTRIBUTED SYSTEMS GROUP

Research Questions

What is the current state of the art of development of incident management/ detection in Cloud-based Big Data analytics and what are the next steps to improve it?

What are current challenges that organisations experience when they are trying to establish incident management in an environment where Big Data applications analyse IoT data on top of hosted Cloud Services?

Stakeholders and Use Cases

Various stakeholders are involved in the operation of the Cloud-based Big Data analytics application but the incident management lacks a conclusive End-to-End view of the whole system involved in Cloud-based Big Data analytics.

Identification and description of relevant, highly generalised use cases helped identify the stakeholder roles and actors and their interaction regarding Incident Management.
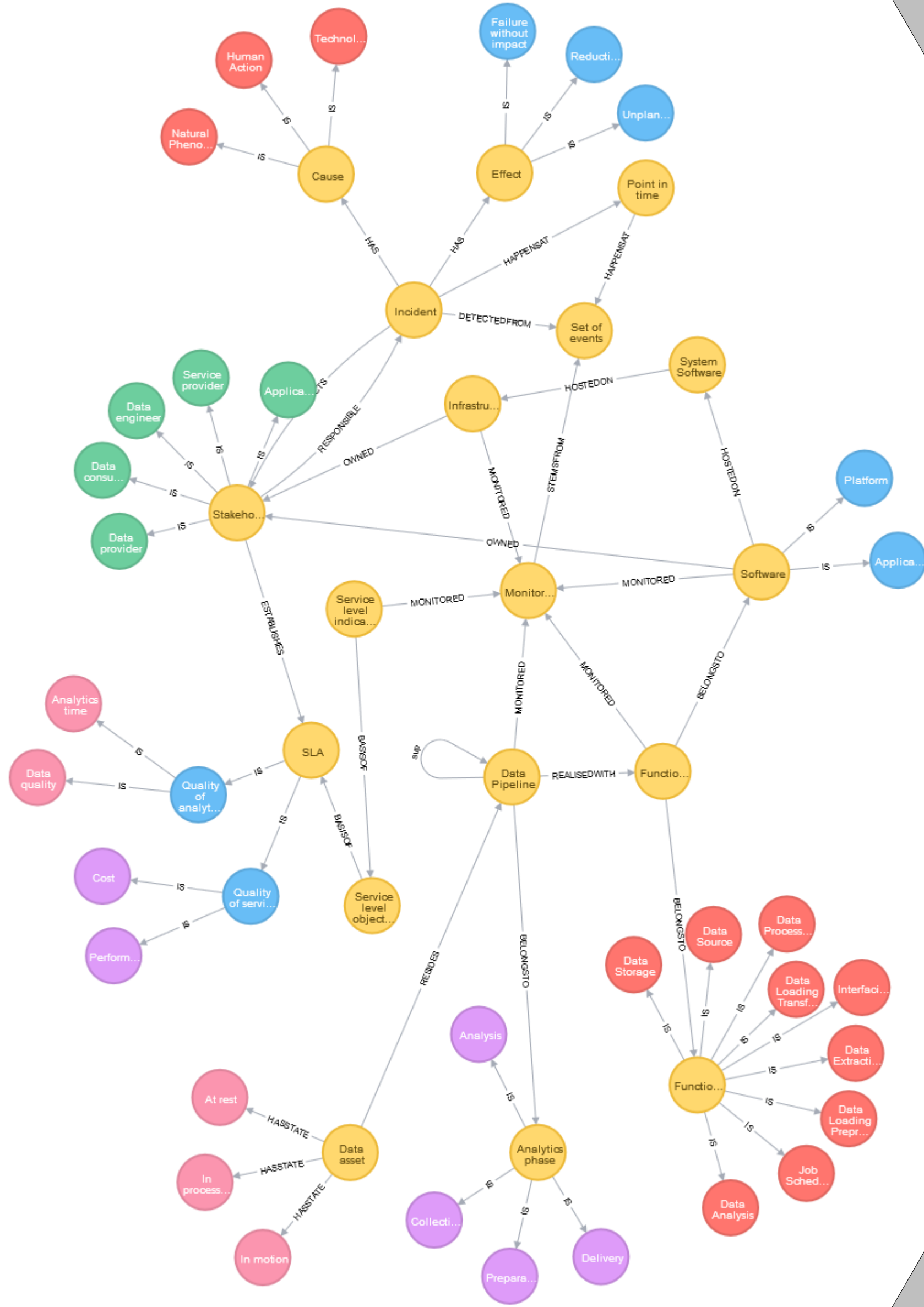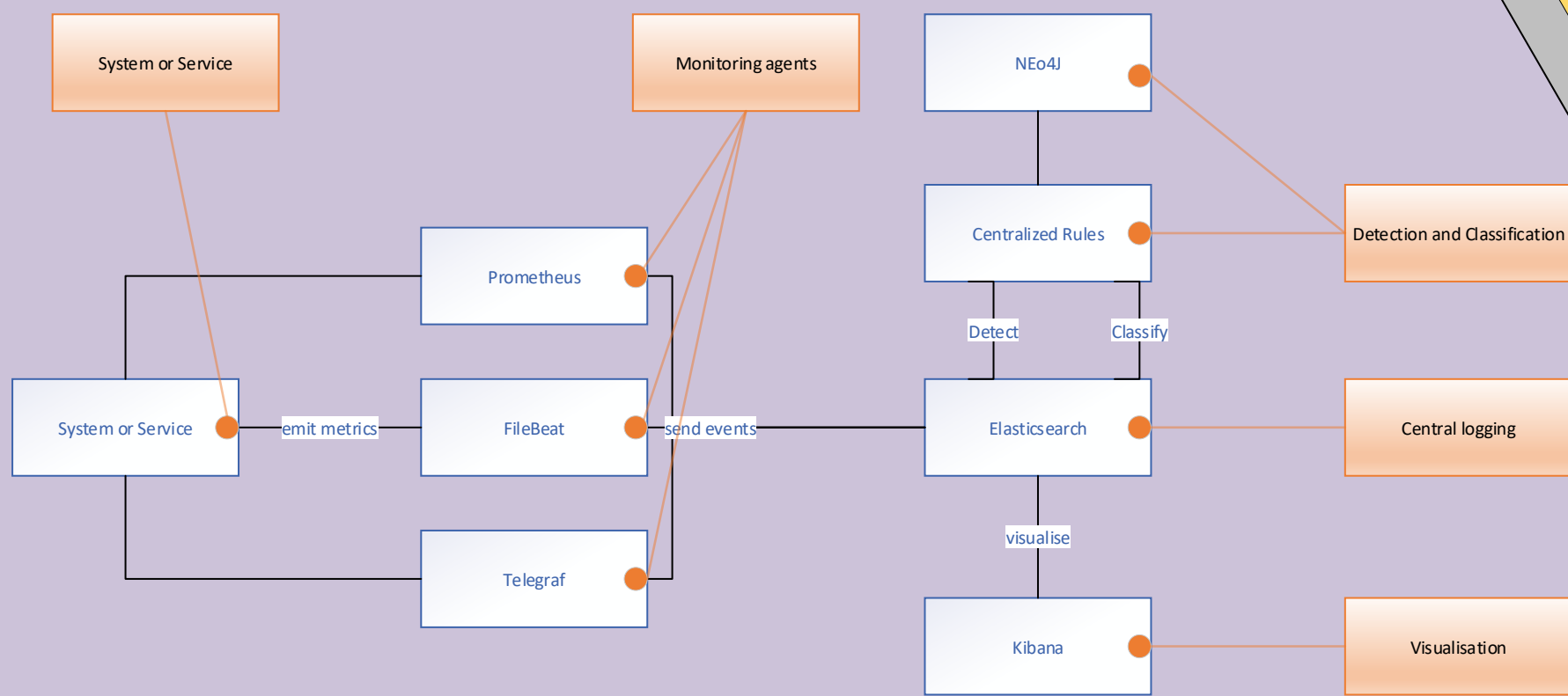

Motivating Scenario

Base Transceiver Stations, forming a large-scale geo-distributed system, providing network to millions and producing massive amounts of data that are processed in Cloud-based Big Data analytics. Incidents are identified too late in the process and oftenonly by human agents.

Classification

The results from the intensive related work and background research, the incident survey and the identification of stakeholders and use cases delivered the input for a graph based classification of incidents.

The graph visualises a generic view of a Cloud-based Big Data analytics application by illustrating a reduction of the complexelements to the essentials needed for incident management.

Incident Survey

A survey of high level incidents regarding Quality of Analytics and Quality of Service was conducted to lay the groundwork for a classification and generic architecture.

The definition of the what, where, when and how of incidents delivered input regarding possible abstractions of Cloud-based Big Data analytics applications and identified key points regarding the interaction of different components.

Architecture

An architecture based on the classification and background research regarding Monitoring, describes in software component diagrams the essential parts of an incident management system and their interaction.

A proof-of-concept was implemented with existing technology to prove the feasibility of the architecture and deliver an source for further studies and expansions.

Conclusions

The identification of use cases and stakeholders, the incident survey, the generic software components, the classification graph and the proof-of-concept deliver a solid foundation for the design and implementation of concrete architectures in the future.