Incident Management in a Software-Defined Business: A Case Study

Eileen Kapel, Luís Miranda da Cruz, Diomidis Spinellis & Arie van Deursen

Abstract

An incident management process is essential in businesses that depend strongly on software and services. A proper process is essential to guarantee that incidents are well-handled, especially in a software-defined financial services company needing to adhere to guidelines and regulations. This paper aims to improve the understanding of the current state of practice through a case study of the incident management process on the software-defined company ING. We conducted the single-case exploratory case study by interviewing 15 subject matter experts on how tools are used, the challenges experienced and the future opportunities of the process. The findings are triangulated with documentation and data.

Research Design

1. Recording of the interview and concurrent note taking
2. Reflective journaling immediately post-interview
3. Reviewing the recording and revising fieldnotes
4. Content analysis: thematic review
5. Triangulation
6. Data Analysis

Tools Usage

The incident management process prescribes tools to be used for incident management & access management and offers flexibility in additional tooling (monitoring, dashboards & documentation) for teams. Besides timely resolution, demonstrable regulatory compliance is a key driver in the process.

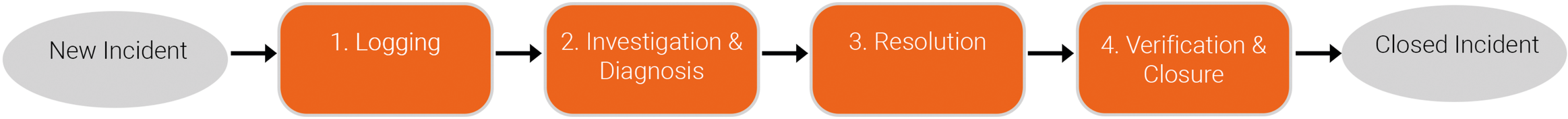
The Main Challenges When Handling Incidents

Logged incidents often consist of false positives and duplicates. They pose big challenges to the subsequent incident management process stages, yet it is not trivial to avoid them.

Good communication is vital in incident management to ensure that each impacted party receives the right form of information in a timely manner. Also, a need is present for guarding the way of working in the process to ensure responsibility for a proper resolution of all incidents.

To comply with risk guidelines for banking an access management tool is employed that lengthens the time to resolve. Each access request needs to be meticulously evaluated, which can be a problem for engineers needing to solve the incident as soon as possible.

The Incident Management Process



It is important to have a complete overview of the whole company to investigate and diagnose the cause of an incident. However, the fast-changing nature and complexity of a large-scale software organisation pose major obstacles in this task.

Unlike the major incident management process, the incident management process tends to focus more on incident resolution rather than on procedural guidelines. The administration of incident tickets is interpreted in different ways amongst stakeholders, leading to inconsistent reports.

Future Opportunities

Enabling automation requires the use of best practices, periodic reviews, clean monitoring data and tight supervision.

Automated resolutions aid the incident management process by automatically fixing incidents without human intervention. This automation should be monitored.

Machine learning on incident and/or monitoring data is a future opportunity for the incident management process to be more automated. This includes anomaly detection for earlier detection of incidents, pattern recognition to learn related incidents and clustering incoming incidents with historical incidents for a faster time to resolve. The success is dependent on the quality of the incoming data and a good overview of the IT environment.

ING TU Delft

e.kapel@tudelft.nl
linkedin.com/in/eileenkapel/

AI FOR FINTECH RESEARCH