ARTMX

Automation of Cloud Abuse Report Handling

Graduate

Anina Bytyçi

Myriam Assunção

Advisor
Prof. Dr. Mitra Purandare

Co-Examiner
Dr. Claudiu Duma, Credit Suisse, Zürich, ZH

Subject Area
Security, Software, Miscellaneous

Project Partner
IBM Research, Rüschlikon, Zürich

Introduction: In recent years, cyber security attacks have become an important issue in the Internet world. There are various attacks such as phishing, malware, denial of service, etc. that aim to breach data.
Public cloud providers are most affected with issue and have to deal with it. Therefore, each cloud provider has a point of contact where issues or suspicious activity in the cloud can be reported via email, and each of these reported issues is analysed and investigated.
IBM Cloud has a dedicated team of analysts who analyse incoming reports of various types of suspected abuse in the cloud. The process of analysing the reports and deciding on the next steps consists of many repetitive tasks that are very time-consuming for any analyst. This is where an automated solution is needed to save valuable time.

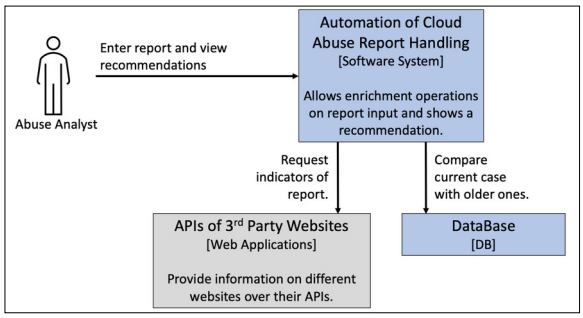
Approach: The goal of this bachelor thesis is to implement a proof-of-concept that automates the manual and time-consuming tasks performed by analysts. At the beginning of the project, a detailed analysis and elaboration was performed, collecting all requirements together with the main stakeholder of the project, IBM Research Zurich. After prioritising the features to be implemented, implementation was started in the construction phase.
Throughout the project, regular meetings were held with stakeholders to receive feedback and new suggestions for improvement. The proof of concept created as the final product was then presented as a demo to analysts at IBM Cloud.

Result: As a result, a web application is developed where key information extracted from reports manually from emails is entered on the user interface. This information is then analysed and enriched on the backend of the product using an external API. The enriched information is then displayed on the user interface along with a screenshot of the suspicious website provided by an additional external API.

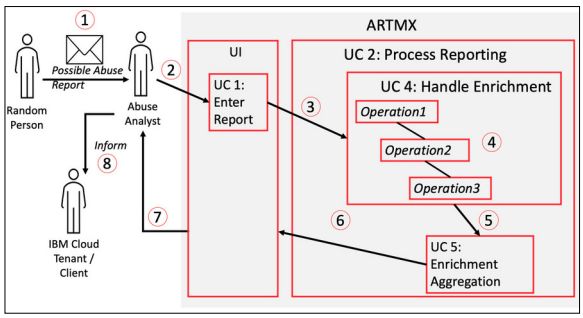
Considering different types of information such as hashes, domain names etc. that can be extracted from reports, a major focus of this project was to build a flexible architecture for the product that would allow it to be easily extended in the future and add new functionality for new indicator types. This was achieved via message queues and task workers in the backend.

Keywords: Cloud abuse reports, Enriched reports, Security analysis, FastAPI, React, MongoDB, RabbitMQ, Celery, VirusTotal API, Screenshot API

Context Diagram
Own presentment



Process Flow
Own presentment



Container Diagram with all used technologies
Own presentment