

Quality ICT B.V.

Client

Research Proposal

Christopher Sulistiyo (4850025)

Christopher.sulistiyo@student.nhlstenden.com

ICT & IC Information Technology Department Emmen

Version 1.1 – 21/02/2024

[Version control 2](#_Toc158708102)

[Remarks 2](#_Toc158708103)

[Introduction 3](#_Toc158708104)

[Reasons for the Research 3](#_Toc158708105)

[Research Objectives 4](#_Toc158708106)

[Main and Sub-Questions 5](#_Toc158708107)

[Concept Theory 6](#_Toc158708108)

[Research Setup 7](#_Toc158708109)

[Design/ Data Collection 7](#_Toc158708110)

[Population and Sample 7](#_Toc158708111)

[Analysis Proposal 8](#_Toc158708112)

[Internal & External Validity and Reliability 8](#_Toc158708113)

[Usability 8](#_Toc158708114)

[Research Tasks 9](#_Toc158708115)

# Version control

|  |  |  |
| --- | --- | --- |
| **Version** | **Activities** | **Date** |
| Initial version 1.0 | Draft version | 06/02/2024 |

Remarks

Any changes and new developments that have a significant impact on the project proceedings will be noted here.

# Introduction

## Reasons for the Research

Q-ICT is a small cybersecurity consultant company based in Emmen, Drenthe, the Netherlands, with clients ranging from small to medium businesses sized companies with employees ranging from 1-100. It currently manages numerous third-party APIs without a standardized implementation within its internal application, the QaaS app. Those APIs are listed in the following:

* **Snelstart**: is used for company’s automation of financial and accounting system software, such as managing invoices, etc,
* **N-Central**: is used for monitoring the clients’ devices. It is a RMM (Remote Monitoring and Management) platform designed to help MSPs (Managed Service Providers) and IT professionals to remotely monitor, manage, and support their clients’ IT infrastructure.
* **Pax8**: is used for their Microsoft subscription. It is a software that helps Q-ICT to simplify the way to buy, sell, and manage cloud solutions.
* **Bodyguard.io**: used for security tab. It is a software developed by a Dutch company to filter and scrutinize downloads from web browsers to detect and prevent malicious files with real-time download scanning capabilities. This API is still relatively newly added by the company,
* **PerfectView**: is a CRM (Customer Relationship Management) from a Dutch company for its solution to help manage, track, and store information related to QICT’s current and potential customer.

These third-party APIs are crucial within Q-ICT, which jobs include offering and advising best solutions and practice for their clients’ IT infrastructure by performing security scans and monitoring their devices health. The functionalities of these third-party APIs are included in the following, but not limited to:

* Monitoring endpoint security events and health status to ensure the effectiveness of security measures.
* Manage and provision cloud-based security solutions to protect client infrastructure and data in the cloud.
* Automate security operations and incident response to efficiently address security threats and vulnerabilities.
* Provide a comprehensive cybersecurity solution tailored to the specific needs and constraints of SMB (Small to Medium Business) clients, enhancing their overall security posture.

Currently, the QaaS app does not have a way to manage their numerous third-party APIs without a standardized implementation. This resulted in a lack of user-friendliness, slow and unclear navigation and data visualization, and the difficulty to integrate a new potential API that might be beneficial to the company. The company consequently seeks to implement a new component within the QaaS app, with functionalities and features such as establishing comprehensive monitoring of these internal APIs, ensuring connection status, error handling, handling of expired API keys, secure storage of keys, and external validation of API connections. Q-ICT, therefore, has asked the author to conduct research regarding the industry-standard best practices for developing and implementing this new component to the QaaS app, while keeping in mind the potential impact of this implementation to its existing operational efficiencies, cybersecurity posture, and end-users’ perceptions and interactions with already existing functionalities in the QaaS app. Furthermore, Q-ICT also seeks to implement SentinelOne API, a new AI powered cybersecurity platform for cyber threat detection and remote IT infrastructure management yet to be explored by the company to the QaaS app. The author is also therefore asked to make a way for the QaaS to be able to necessitate interpreting the all the APIs’ response in the form of XML and JSON files.

## Research Objectives

The objectives of this research are listed in the following:

* **API monitoring best practices**: the result of this research is to find and identify best practices for API monitoring functionality into an existing application. It will prioritize these functionalities necessary for developing the proposed solution. This includes real-time monitoring, error detection, and insight generation regarding API connections.
* **Integration with SentinelOne**: this research will also explore how SentinelOne can be integrated into the QaaS app to align with API monitoring functionality while leveraging its key features for cyber threat detection and remote IT infrastructure management.
* **Best visualization techniques**: this research will also propose suitable visualization techniques for displaying data processed and received by the internal application in XML and JSON formats, focusing on clear and insightful representation of threats detected by all the APIs listed above and SentinelOne.
* **Potential data integrity issue**: furthermore, this research will deal into potential impact assessment in implementing SentinelOne to already existing APIs like N-Central. This involves assessing how the implementation of the proposed solution can improve overall performance, cybersecurity measures, and user experience.

## Main and Sub-Questions

A research main question is a crucial component when doing research as it serves as the driving force behind the study, guiding the research process, structuring the paper, promoting clarity, driving inquiry, addressing relevance, and facilitating evaluation. The main research question is as follows:

*“How can Q-ICT effectively enhance API monitoring within its internal application while integrating and leveraging SentinelOne security threat platform for continuous cybersecurity monitoring while still ensuring adherence to the highest security standards?”*

The research sub-questions are crucial in shaping the research process and facilitating the thorough investigation and eventual answer to the main question. They are as follows:

* What is the current situation of the QaaS app, the internal application used within Q-ICT to monitor its third-party API calls?
* What functionalities should be prioritized in the development of monitoring and managing third-party APIs within an internal application while ensuring real-time monitoring, error detection, and insight generation regarding API connections?
* How can SentinelOne be integrated into the environment, specifically aligning with the API monitoring functionality, while still utilizing key features and capabilities in the context of cyber threat detection and remote IT infrastructure management?
* What are suitable visualization techniques for displaying data processed and received by the internal threats detected by SentinelOne and other Q-ICT relevant API connections?

These research questions do not make substantial statements about the research that will be executed and can be later subject to change after a proper consultation with the school supervisor.

## Concept Theory

* Clarify concepts in your central question / stipulative definitions
* Used definitions apply to the knowledge base (best practices/ implicit
* and explicit knowledge)
* Sources within the company or employees

# Research Setup

## Design/ Data Collection

In this research, different research methods have been used to answer the above-mentioned research main question. A research methodology must be defined for each research sub-questions to determine how the results are being considered valid and reliable.

* **Sub question 1**: a combination of desk research (Literature study of the library method of ICT Research Methodology) and Interview (from the Field method of ICT Research Methodology) with the creator of the QaaS app will be conducted, with the goal of understanding the infrastructure beneath along with understanding all its dependencies. The author will then gain a substantial amount of understanding from its Flutter-based code, as well as the Node.js TypeScript based RESTful API server behind it, and the Firebase from GCP (Google Cloud Platform) services and functionalities being used within the QaaS app such as Google Secret Manager, Firebase, Cloud Functions, Firestore, Google Authentication, Cloud Messaging, Cloud Storage, Google Analytics, hosting services, real-time databases, etc,.
* **Sub question 2**: the type of data collection that will be used are observation and interviews with the product owner and stakeholders.
* **Sub question 3**: this sub-question will be answered by doing experimental activities, creating reports, and doing desk research. The SentinelOne Internal API documentation will be used as selected measuring instruments.
* **Sub question 4**: this sub-question will also be answered by doing desk research, observation, experimentation, and reporting to the company supervisor and stakeholders.

## Population and Sample

Population refers to the entire group of individuals and/or entities that the research aims to study. The population of this research mainly consists of a group of individuals ranging from high school students to any graduate from academic degree that are interested in the fields of IT, especially regarding API connections and best cybersecurity practices.

Sample represents a subset of population that is selected for the actual study. In this case, the sample would be the Software Development departments of Q-ICT B.V. itself and the teachers and supervisors of NHL Stenden Hogeschool of the ICT & IC Information Technology department in Emmen where the author is conducting this research for.

## Analysis Proposal

Within this graduation process, the author aims to study and assess the existing internal application code and features crafted using Flutter for the front-end and Node.js for the server back-end. It seeks to meticulously analyse these components to identify any undisclosed bugs, assess their weaknesses and strengths, and evaluate any potential security vulnerabilities. Additionally, the author intends to explore opportunities for enhancements, identify areas for refinement, and pinpoint potential spaces for development of the proposed features stated in the Graduation Description.

Furthermore, the author endeavours to conduct a comprehensive analysis of Firebase as a cloud solution, examining its full suite of services offered, in order to ascertain the most suitable offerings to integrate for the proposed new features within the framework of the existing internal application for the graduation assignment.

## Internal & External Validity and Reliability

The reliability is validated by interviewing the developers behind the QaaS app, incorporating any feedback to the application that they might give while the author is trying to implement this new feature. To further improve validity, the business and product owner, and additional stakeholders of Q-ICT will also later be questioned to achieve the desired outcome of the new component requested.

## Usability

The usability of a research is often determined by the relevance and clarity of its main and sub-questions. It can be assessed as in the following:

* **Practical Implementation**: the results of this research will later be used to generate actionable insights and guidance during the Realization phase of the graduation work placement by the author. The Research Report as the end-result of this research will also provide recommendations to Q-ICT regarding the research topic.
* **Consideration of Best Cybersecurity and Industry Standards**: the inclusion about the needs to implement the best cybersecurity and industry standards demonstrates an awareness of the importance of aligning the research with those existing standards. This consideration enhances the practical applicability and usability of the research in the broader context of industry norms.
* **Impact Assessment**: the research will also discuss about the potential impact on integrating this new component on the operational level of the QaaS app product, indicating an intention to evaluate the practical consequences of the proposed solution. This focus on impact enhances the usability by providing insights into potential benefits and challenges of the main research question.

# Research Tasks

The tasks that the author will undertake whilst doing this research are planned and included in the following:

* Interview with the developers behind the QaaS app.
* Interview with the owner of the Q-ICT.
* Interview with the additional 2 stakeholders of Q-ICT.
* Review the Flutter client-side front-end and Node.js server-side back-end code, as well as understanding all the Firebase functionalities used within the internal application.
* Review and study all the listed 5 APIs and SentinelOne API documentations.
* Conduct desk research regarding all the research sub-questions listed above.