Research Proposal

Christopher Sulistiyo (4850025)

Christopher.sulistiyo@student.nhlstenden.com

ICT & IC Information Technology Department Emmen

Client

Quality ICT B.V.

Version 1.1 – 21/02/2024

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 (SME (small and medium-sized enterpirses) in English or MKB (midden- en kleinbedrijf) in Dutch) 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,

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:

- **Integration with SentinelOne**: this research will also explore how SentinelOne can be integrated into the QaaS app to align with other modules of the QaaS App while leveraging its key features for cyber threat detection and remote IT infrastructure management.
- **Best visualization techniques for SentinelOne data**: 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 SentinelOne API.

- **Follow code conventional guidelines, maintain best cybersecurity practices, and unit testing**: during the development of the final product, the Company Supervisor wishes that the author follow the best code conventional style with MVC architectural style that was already implemented on the QaaS app, as well as following the best cybersecurity standards and implementation of unit testing in both Flutter front-end and Firebase back-end code.

Research 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 integrate and leverage SentinelOne security threat platform for continuous cybersecurity monitoring?"

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, alongside its back-end infrastructure?
- How can SentinelOne be integrated into the QaaS app, 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 Security Threat Platforms regarding to SentinelOne APIs compares to other visualization techniques by the same platform?

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

Concept clarification

In this graduation research, the central question revolves around integrating the SentinelOne security threat platform for continuous cybersecurity monitoring, all while ensuring adherence to the highest security standards. To elucidate this question further, it is imperative to provide stipulative definitions for the key terms and concepts involved in this study.

Firstly, the "SentinelOne security threat platform" encompasses a well-known comprehensive cyber security solution from United States of America designed to detect, prevent, and respond to various security threats within Q-ICT's IT infrastructure powered by AI. This platform utilizes advanced threat detection algorithms, machine learning capabilities, and real-time monitoring to safeguard against cyber threats such as malwares, ransomwares, phishing emails, and unauthorized access attempts.

Secondly, "continuous cybersecurity monitoring" denotes the ongoing process of monitoring and analysing Q-ICT's IT environment for potential security vulnerabilities, breaches, or anomalous activities. This involves real-time monitoring of network traffic, system logs, user activities, and application behaviour to proactively identify and mitigate security risks.

Furthermore, "adherence to the highest security standards" encompasses the implementation of industry best practices, regulatory compliance requirements, and robust security measures to ensure the confidentiality, integrity, and availability of Q-ICT's internal application and data. This includes adhering to the standards such as ISO 27001, NIST cybersecurity framework, and GDPR regulations to mitigate security risks and protect sensitive information.

Definitions to apply to the knowledge base.

Definitions used in the research:

Real-time monitoring: the continuous tracking and analysis of API interactions within Q-ICT's internal application to detect and respond to events as they occur, ensuring timely identification of anomalies or security threats.

Error detection: the process of identifying and flagging any deviations, discrepancies, or failures in API transactions within the internal application, facilitating prompt resolution and maintaining system integrity.

Insight generation: the extraction and analysis of data from API connections to gain actionable insights and inform decision-making processes related to system performance, user behaviour, and security posture.

Cyber threat detection: the process of identifying, analysing, and responding to potential security threats within Q-ICT's IT infrastructure, including those originating from third-party API interactions, utilizing SentinelOne's advanced threat detection capabilities.

Remote IT infrastructure management: The ability to remotely monitor, configure, and manage Q-ICT's IT infrastructure, including API endpoints and security measures, leveraging SentinelOne's centralized management features and remote access capabilities.

Data visualization: methods used to present complex data in a visual format that is easy to understand and interpret, facilitating insights and decision-making. Examples include pie charts, charts, graphs, figures, pictures, and heatmaps in the dashboard.

Internal threats: security risks originating from within Q-ICT's IT infrastructure, including potential vulnerabilities, unauthorized access attempts, and anomalous activities detected by SentinelOne, other third-party APIs, and other security measures.

SentinelOne data: information collected and processed by SentinelOne regarding detected cyber threats, including threat types, severity levels, affected systems, and response actions.

Q-ICT relevant API connections: third-party API interactions within Q-ICT's internal application, including data exchanges, system integrations, and communication channels.

Knowledge Base Application

Before proceeding any further, it is important to know what the definitions of implicit/tacit and explicit/expressive knowledge are. Below are the given definitions:

Implicit knowledge: is a knowledge that is gained through incidental activities, or without awareness that learning is occurring. (*Wikipedia, n.d.*). It helps individuals differentiate themselves from other candidates. When an organization has a wide scope of tacit

knowledge, it can rely on its talented pool of employees to develop innovative solutions, thus helping the organization to become industry leaders. An organization can also recognize its tacit knowledge and develop the appropriate resources to train new hires as effectively as possible.

Explicit knowledge: is a knowledge that is straightforwardly expressed and shared between people (*Wikipedia, n.d.*). It can help employees within an organization share valuable information with their coworkers or customers. Transferring explicit knowledge to others in the workplace allows employees to learn new information that can help them do their jobs effectively.

Best practices:

- The integration of SentinelOne allows for comprehensive threat detection and response capabilities, ensuring the protection of API connections and IT infrastructure against cyber threats. This will algin with the industry best practices to enhance overall security posture.
- Data visualization emphasizes the use of intuitive and interactive visualization techniques to present complex cybersecurity data effectively. This includes techniques such as interactive dashboards, dynamic charts, and hierarchical visualizations that enable users to explore and analyse data related to internal threats by SentinelOne and other API connections.

Implicit knowledge:

- Employees within Q-ICT may process tacit knowledge regarding effective visualization techniques that have been successful in previous cybersecurity initiatives or similar projects. Leveraging this knowledge can inform the selection of visualization techniques tailored to Q-ICT's specific needs and preferences.

Explicit knowledge:

- Technical documentation and case studies from SentinelOne can provide insights into the platform's key features and capabilities relevant to cyber threat detection and remote IT infrastructure management. This explicit knowledge can guide the

integration process and help maximize the utilization of SentinelOne Q-ICT's environment.

- Resources such as academic literatures and case studies provide insights into the best practices and emerging trends in cybersecurity data visualization. This explicit knowledge can guide the selection of suitable visualization techniques that align with industry standards and facilitate effective communication of internal threat data to stakeholders within Q-ICT.

Application

Based on the definitions stated above and its knowledge base application, some example implementation can be drawn up regarding the graduation work placement project.

Sub-question #2:

To answer this sub-question, Q-ICT should strategically integrate SentinelOne into its environment, ensuring alignment with other module functionalities while leveraging key features for cyber threat detection and remote IT infrastructure management. By integrating SentinelOne's threat detection tools, Q-ICT can therefore enhance its ability to detect and respond to cyber threats originating from API connections in real-time. Additionally, leveraging SentinelOne's centralized management features enables remote monitoring and management of Q-ICT's IT infrastructure, including API endpoints, ensuring consistent security across the organization's digital ecosystem.

Sub-question #3:

To address this sub-question, Q-ICT should explore suitable visualization techniques for displaying data processed and received by internal threats detected by SentinelOne and other relevant API connections. Interactive dashboards can be used to provide an overview of detected threats, allowing users to drill down into specific details such as threat types, affected systems, and response actions. Dynamic charts and graphs can visualize trends and patterns in threat data over time, helping stakeholders identify emerging threats and prioritize mitigation efforts. Additionally, heatmaps can highlight areas og high threat activity within Q-ICT's IT infrastructure, guiding targeted security measures. By leveraging these visualization techniques, Q-ICT can effectively communicate internal threat data to

stakeholders and facilitate informed decision-making regarding cyber security strategies and resource allocation.

Sources validation within the company or employees

Lastly, for the validation of the sources within the company or employees, the interviews that will be conducted by the author will be primarily addressed to the developers of the QaaS app, the company owner, and stakeholders. Their respective name will be Manuel Weidijk as Q-ICT senior software developer, Mark Kolk as the owner of Q-ICT, and Pierre Kleine Schaars, Luke Admiraal, Pete Hoekstraa, and Bas Ter Heurne as the stakeholders of Q-ICT, along with its sister companies, MKBiT and QaaS (Quality as a Service).

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 (*Wikipedia, n.d.*). 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 (*Wikipedia, n.d.*). 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, 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.