Thesis

NHL Stenden University of Applied Sciences

In the department of:

ICT & CT Information Technology Bachelor Emmen

In association with:

Q-ICT B.V.

Written by:

Christopher Sulistiyo (4850025)

Submission:

1-August-2024

Work placement lecturer(s):

Company Supervisor(s): Manuel Weidijk
Mark Kolk

Summary

Contents

List of Figures

Glossary

CRM is a technology for managing all your company's relationships and interactions with customers and potential customers. It provides a centralized DB or system for storing and organizing customer data, as well as tools for managing sales, marketing, customer service, and other aspects of customer realationships. A CRM system helps companies stay connected to customers, streamline processes, and improve profitability (Wikipedia, n.d.-b) . 9

Pentest A.K.A. ethical hacking, is a simulated cyberattack where professional ethical hackers break into corporate networks to find weaknesses (Wikipedia, n.d.-d) . 6

Acronyms

AI Artificial Intelligence. 5, 9

APA American Psychological Association. 7

API Application Programming Interface. 5, 7–9

B.V. Besloten Vennootschap. 0, 5

BaaS Back-end as a Service. 9

CRM Customer Relationship Management. 9

CSF Cybersecurity Framework. 5

CT Creative Technology. 0

FIPS Federal Information Processing Standards. 5

GCP Google Cloud Platform. 9

ICT Information and Communication Technology. 0, 8

ISO International Organization for Standardization. 6

IT Information Technology. 5–7, 9

ITIL Information Technology Infrastructure Library. 6

JSON JavaScript Object Notation. 8

MSP Managed Service Provider. 9

NIST National Institute of Standards and Technology. 5, 6

OS Operating System. 9

Q-ICT Quality ICT. 0, 5, 6, 8–10

QaaS Quality as a Service. 7–9

RRM Remote Monitoring and Management. 9

SIEM Security Information and Event Management. 6

SME Small and Medium-sized Enterprises. 5, 9

UI User Interface. 9

XML Extensible Markup Language. 8

Chapter 1

Introduction

1.1 Project Background

In today's rapidly evolving digital landscape, cybersecurity remains a paramount concern for organizations across all industries. With the proliferation of sophisticated cyber threats and the increasing complexity of IT infrastructures, business are constantly seeking new and innovative ways to protect their digital assets and fortify their defences and safeguard sensitive data. In this pursuit, cybersecurity consultant firms have emerged as a critical ally for organizations, providing expert guidance and support in the development and implementation of robust cybersecurity strategies, playing a pivotal role in offering expertise and guidance to help organizations navigate the intricate realm of cybersecurity.

One of the key strategies employed by cybersecurity consultants is the integration of third-party security APIs into their arsenal of tools and technologies. These APIs provide invaluable functionalities, ranging from vulnerability assessment and security scans to device health monitoring and threat intelligence analysis by AI. By leveraging these APIs, cybersecurity consultants can enhance their capabilities and provide a more comprehensive and effective security solution to their clients, streamline their operations, provide clients with robust, proactive security measurers, and improve their overall service delivery.

1.2 The Company and the QaaS App

Q-ICT B.V., is a small cybersecurity consultancy based in Emmen, northeast of the Netherlands. It recognizes the critical importance of proactive API monitoring in safeguarding its clients' digital assets. Their customers are SME companies with employees ranging from 1 to 100. Q-ICT is therefore asked to monitor their clients' devices and ensuring the overall security of their systems, IT infrastructure, and digital assets. They typically engage in various activities, including:

- **Continuous Monitoring and Maintenance**: implementing tools and processes for continuous monitoring of clients' systems, devices, networks, and systems to detect and respond to security threats in real-time and address emerging threats and vulnerabilities.
- **Vulnerability Assessment**: conducting regular vulnerability assessments and penetration testing to identify weaknesses in clients' systems and infrastructure
- **Incident Response**: developing and implementing plans and protocols for responding to and mitigating cybersecurity incidents effectively and efficiently.
- **Penetration Testing**: simulating cyberattacks to identify weaknesses in the client's defences and assess their ability to withstand and respond to real-world cyber threats.
- **Security Incident Investigation**: conducting thorough investigations into security incidents to identify the root cause and impact of the incident and develop strategies to prevent future occurrences.

1.2.1 Working Methodology

The company currently utilizes the five functions defined by NIST as part of its CSF as the framework to help the company manage and improve their cybersecurity risk management processes. These five functions are part of the FIPS 199. All functions serve as level categories for organizing cybersecurity activities within an organization and are as follows (NIST, 2023):

- **Identify**: develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This includes the development of an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It also includes the development of a cybersecurity risk

management strategy that is aligned with the organization's mission, goals, and objectives and the establishment of a governance structure to ensure that the strategy is effectively implemented and maintained.

- **Protect**: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. It can help the company assists clients in implementing security controls, encryption mechanism, access controls, and other security measures to protect their systems and data from unauthorized access, disclosure, and alteration or modification.

- **Detect**: develop and implement the appropriate activities to identify and detect the occurrence of a cybersecurity event in timely manner to facilitate rapid response and mitigation efforts. This includes the development of a cybersecurity event detection capability that is integrated with the company's incident response and recovery capabilities. It will help the company to implement monitoring and detection mechanisms, such as intrusion detection systems, log analysis tools, and SIEM systems, to detect and identify to cybersecurity incidents promptly.

- **Respond**: develop and implement the appropriate activities to take action in responding regarding a detected cybersecurity event, containing the impact, and restoring normal operations. It involves activities such as developing incident response plans, conducting incident response drills and exercises, establishing communication channels with stakeholders, and implementing recovery strategies to minimize the impact of cybersecurity incidents on business operations and services.

- **Recover**: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident and event, along with implementing improvements to prevent future incidents. In this activity, the company should be able to develop and implement recovery plans, conduct post-incident reviews and analysis, identify areas for improvement, and implement measures and improvements to enhance resilience and prevention future incidents.

Furthermore, the company also uses the ISO 27001 as the main standard for information security management and the NIST 800-53 as the main standard for security and privacy controls for federal information systems and organizations.

1.2.2 Departments

The company consists of multiple departments in its behalf, each with their own functions and responsibilities. Those departments are the following:

1. *Service Help Desk Department*: it serves as a frontline support function responsible for addressing client inquiries, troubleshooting technical issues, and providing guidance and support to clients in resolving their technical challenges. It contains 2 subdepartments, the first level help desk and the second level help desk. The First Level Help Desk is the first point of contact for clients seeking technical assistance and support, and it is responsible for managing and resolving client issues in a timely and efficient manner. The Second Level help desk is responsible for providing more advanced technical support and troubleshooting for complex technical issues and consists of Senior System Engineers. It has 2 services, mainly the indoor and outdoor customer services. With the indoor customer services, the company provides remote support to clients, while with the outdoor customer services, the company provides on-site support to clients.

2. *Cybersecurity Department*: it's responsible for implementing procedures that will be used throughout the company's system, especially in Help Desk Department, to ensure that the company's information technology infrastructure is secure. It also develops methodologies and best practices related to cybersecurity, as well as integrating ITIL principles and product management practices into the company's operations. Conducting regular security scans for clients' networks, systems, and applications to identify vulnerabilities and security risks, and performing Pentest that involves simulating cyberattacks to identify weaknesses in the client's defences and assess their ability to withstand and respond to real-world cyber threats. This department mainly consist of IT managers, pentesters, and cybersecurity specialists.

3. *Software Development Department*: it addresses Q-ICT clients needs by creating custom software solutions tailored to their specific requirements. It consists of software developers that work closely with clients to understand their unique cybersecurity challenges and design solutions that effectively address those concerns, while utilizing their expertise in programming languages, software frameworks, and cybersecurity principle to develop secure and reliable applications. This is the department where the author is currently working in his graduation work placement project. Mainly, this department uses Dart with Flutter as the main front-end development framework, and Node.js with TypeScript template as the main back-end development framework. Furthermore, it utilizes Google Firebase as the main cloud solution for the applications it develops as it works hand-in-hand with Flutter, but it expresses its desires to expand more into Microsoft Azure in the future.

4. *Financial Department*: it is responsible for managing the financial aspects of the company to ensure its financial health and stability. It includes Accountant and Financial Advisor, and they are responsible

for analyzing financial data, identifying trends, and making strategic financial decisions to support the company's growth and objectives.

1.3 Problem Statement

The company currently manages numerous third-party APIs for the above-mentioned purposes. Currently, those APIs are managed manually and without a standardized implementation in their internal application, the QaaS app, which is a time-consuming and error-prone process. This has led to several problems, namely:

- Inefficient and fragmented approach to API management.
- Lack of user-friendliness, and slow and unclear navigation.
- Inconsistent integration of APIs into the application.
- Poses a significant challenge in error handling and debugging, as disparate error reporting mechanism across the APIs hinder efficient troubleshooting and resolution processes.
- Difficulty to maintain and update APIs.
- Lack of clear and concise documentation.
- Lack of a centralized API management system.
- Inadequate security measures, as the company risks inconsistent data retrieval and analysis across its APIs, potentially leading to incomplete insights into client IT systems and infrastructure.

Thus, the company has tasked the author with the development of a standardized API monitoring system within the QaaS app, with features such as error handling, connection status warranty, debugging, and the effective integration of the SentinelOne security threat platform for continuous cybersecurity monitoring within the QaaS app as the main topic of his graduation work placement project.

1.4 Project Objectives

In the end of this project which consist of 90-99 working days, the following objectives should be achieved:

1. Develop a standardized API monitoring system within the QaaS app, with features such as error handling, connection status warranty, debugging, .
2. Effectively integrates and leverages the SentinelOne security threat platform for continuous cybersecurity monitoring within the QaaS app.

1.5 Reading Guide

This report is structured as follows:

- **Summary**: provides a brief and concise overview of the entire report, including the research questions, key findings, and conclusion. Its purpose is to provide readers with a quick and comprehensive understanding of the report.
- **Introduction**: provides an overview of the project background, the research topic the company, and the project objectives. It introduces the context of the research and outlines the structure of the report.
- **Research**: presents the research results, including the research methodology, the findings, and the analysis of the research questions. Firstly, it describes the methodologies employed during the research, and then it provides a detailed account of the research process and the outcomes of the research.
- **Realization**: provides a detailed description of the software end-product developed during this work placement project. It outlines insights into design, development, and implementation phases. It also highlights key features, functionalities, and technology specifications used in the project.
- **Conclusions and Recommendations**: the Conclusion summarizes the key findings and results achieved during the research and realization phases. The Recommendation section outlines the proposed next steps and future research areas to further enhance the project and address any outstanding issues. It discusses potential areas for further exploration or refinement.
- **References**: lists all the sources cited in the report following the appropriate to APA 7th edition citation style.
- **Appendices**: includes any additional supplementary information, data, or materials that are relevant to the report but not included in the main body of the report.

Chapter 2

Research Results

2.1 Research Topic

In a research, it is paramount to have the formulation of a clear research topic, research main question, and research sub-questions. The main question serves as the focal point around which the research revolves, encapsulating the primary objective or purpose of the study. The following main research question will be used throughout the research:

"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 then used to function as a pathway that dissect the main question into smaller, more manageable components, which can then be addressed individually. This approach allows for a more comprehensive and in-depth analysis of the research topic, ensuring that all relevant aspects are covered and that the research is conducted in a systematic and organized manner. This research main question is therefore expanded in the following research sub-questions:

- What is the current situation of the QaaS app of Q-ICT?
- 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 can be integrated into the QaaS app environment, especially aligning with the API monitoring functionality, while still utilizing their key features and capabilities in context of cyber threat detection and remote IT infrastructure management?
- What are the most suitable visualization techniques for displaying the data processed and received by the QaaS app in XML and JSON formats to ensure clear and insightful representation of threats detected by SentinelOne and other relevant API connections?

2.2 Research Methodology

In this research, different research methods have been used to answer the research questions. This research will be based on the six ICT research methods defined by HBO-I (Vogel, 2023). A research method for each sub-question is then defined along with how the results are considered valid and reliable:

2.2.1 Method of Data Collection

- Sub-question #1:
- Sub-question #2:
- Sub-question #3:
- Sub-question #4:

2.2.2 Selected Measuring Instruments

- Sub-question #1:
- Sub-question #2:
- Sub-question #3:
- Sub-question #4: the selected measuring instruments for this sub-question will be through observation and reading the studies of.

2.2.3 Method of Data Analysis

- Sub-question #1:
- Sub-question #2:
- Sub-question #3:
- Sub-question #4:

2.2.4 Reliability, Validity, and General Applicability

- Sub-question #1:
- Sub-question #2:
- Sub-question #3:
- Sub-question #4:

2.3 Research Question #1

The QaaS app is a web application that is used by Q-ICT. It is in Dart with Flutter as the front-end framework.

2.3.1 QaaS App Infrastructure

Flutter

Flutter is an open-source framework made by Google in 2017. It used as an UI toolkit for building natively compiled applications for mobile, web, and desktop (Windows, macOS, Linux) from a single codebase (Wikipedia, n.d.-c).

Firebase

Firebase is a comprehensive platform for developing and managing web and mobile applications, created by Google and is party of GCP. It was originally an independent company founded by Firebase, Inc. in 2011. It was then acquired by Google in 2014. Since then, it has become an integral part of Google's broader ecosystem of cloud services.

Firebase is a BaaS that provides developers with a variety of tools and services to help with both back-end infrastructure and front-end capabilities without worrying about managing servers or infrastructures.

- Firestore Database: Firestore is a NoSQL database that is part of the Firebase platform. It is a flexible, scalable database for mobile, web, and server development. It keeps data in sync across client apps through real-time listeners and offers offline support for mobile and web, so the developers can build responsive apps that work regardless of network latency or Internet connectivity.
- Authentication
- Functions
- Hosting
- Real-time database:

Algolia

Algolia is used for search functionality. It is a search-as-a-service platform that enables developers to integrate and build fast, relevant search functionality into their applications and websites (Wikipedia, n.d.-a). It provides a range of features and capabilities for building and managing search functionality, including full-text search, typo tolerance, and relevance tuning, as well as analytics and monitoring tools to help developers understand how users are interacting with their search functionality in real-time.

The reason as to why Q-ICT uses Algolia is that the nature of Firebase search engine is quite often proven to be inaccurate and slow.

NoSQL Database

2.3.2 Q-ICT Internal APIs

Those APIs are the following:

- Resello: is used for Q-ICT Microsoft subscriptions owned by Pax8. It is a cloud marketplace that simplifies the way SMEs buy, sell, and manage cloud solutions through automation. It provides a single platform to manage the entire cloud customer lifecycle, from quote to cash to support, thus simplifying the process of buying, selling and managing cloud solutions.
- SnelStart: is used for Q-ICT automation of financial and accounting system software, such as managing invoices, etc., for SMEs. It offers a range of products and services to help businesses manage their finances, including accounting software, invoicing software, and financial management tools.
- SentinelOne: is a cybersecurity platform that provides endpoint protection, detection, and response capabilities to help organizations defend against advanced cyber threats. It leverages Artificial Intelligence and machine learning to analyze and respond to security threats in real-time, providing organizations with comprehensive protection against malware, ransomware, and other cyber threats. It also provides visibility into clients' IT systems and infrastructure, enabling organizations to gain insights into potential security risks and vulnerabilities and take proactive measures to address them.
- Bodyguard.io: is used for security tab. It is a product from a Dutch company that filters and scrutinizes downloads from web browsers to detect and prevent malicious files with real-time download scanning capabilities.
- N-Central: is a product from N-Able and is used for monitoring clients' devices and ensuring the overall security of their systems, IT infrastructure, and digital assets. It is a RRM platform designed to help MSP and IT professionals to remotely monitor and manage their clients' devices and networks. It provides a comprehensive set of tools and features for monitoring, managing, and securing clients' devices and

networks, including remote monitoring and management, patch management, antivirus, backup and disaster recovery, and network topology mapping.

- PerfectView: is a CRM application from a Dutch company designed to help manage, track, and store information related to Q-ICT's current and potential customers.
- Computicate:

2.4 Research Question #2

2.5 Research Question #3

2.6 Research Question #4

Chapter 3

Realization

Chapter 4

Conclusion and Recommendation

Bibliography

NIST. (2023). The five functions. *NIST Government*. https://www.nist.gov/cyberframework/online-learning/five-functions

Vogel, J. (2023). Ict research methods — methods pack for research in ict. *HBO-i, Amsterdam*. https://ictresearchmethods.nl/

Wikipedia. (n.d.-a). Algolia. *Wikipedia, free encyclopedias*. https://en.wikipedia.org/wiki/Algolia

Wikipedia. (n.d.-b). Customer relationship management. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Customer_relationship_management

Wikipedia. (n.d.-c). Flutter (software). *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Flutter_(software)

Wikipedia. (n.d.-d). Penetration test. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Penetration_test

Appendix A

Planning

Appendix B

Project Plan

Appendix C

FO (Functional Overview)/SRS(Software Requirements Specification)/PRS (Product Requirements Specification)