Thesis

NHL Stenden University of Applied Sciences

In the department of:

ICT & CT Information Technology Bachelor Emmen

In association with:

Quality 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

Special Terms

AI Artificial Intelligence. 5

API Application Programming Interface. 5–7

ICT Information and Communication Technology. 0, 7

IT Information Technology. 5, 6

Q-ICT Quality ICT. 5, 7

QaaS Quality as a Service. 5, 7

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 Q-ICT Software Development Department

Q-ICT, a small cybersecurity consultancy that the author is currently doing his graduation internship in, recognizes the critical importance of proactive API monitoring in safeguarding its clients' digital assets. Their customers are small to medium-sized business 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 cyber attacks to identify weaknesses in the client's defences and assess their ability to withstand and respond to real-world cyber threats.
- **Secyrity 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.

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:
2. Cybersecurity Department:
3. Software Development Department:
4. Financial Department:

The author of this document is currently working within the software development department under the supervision of 2 people, which are the senior software developer and the cybersecurity specialist.

The company currently manages numerous third-party

APIs for the above-mentioned purposes. Those APIs are the following:

- Pax8:
- SnelStart:
- SentinelOne:
- Bodyguard.io:
- N-Central:
- PerfectView:
- Computicate:

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 a 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..

1.3 Project Objectives

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

1. Develop a

1.4 Reading Guide

Chapter 2

Research Results

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 researchr revolves, encapsulating the primary objective or purpose of the study. The research sub-questions are then used to function as a pathway that dissect The following main research question will be use 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 main question is then expanded in the following research sub-questions:

- What is the current situation of the QaaS app of Q-ICT?
- 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?

2.1 Research Methodology

In this research, different research methods have been used to answer the research questions. This research will 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:

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

2.2 Research Question #1: What is the Current Situation of the QaaS App of Q-ICT?

The QaaS app is a web application that is used by Q-ICT .

2.2.1 QaaS App Infrastructure

Chapter 3

Realization

Chapter 4

Conclusion and Recommendation

Appendix A

Planning

Appendix B

Project Plan

Appendix C

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

Bibliography

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