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 terms **4**

1 Introduction **5**
1.1 Project Background 5
1.2 Q-ICT Software Development Department 5
1.3 Project Objectives 6
1.4 Reading Guide 6

2 Research Results **7**
2.1 Research Methodology 7

3 Realization **8**

4 Conclusion and Recommendation **9**

A Planning **10**

B Project Plan **11**

C FO (Functional Overview)/SRS(Software Requirements Specification)/PRS (Product Requirements Specification) **12**

List of Figures

Special Terms

AI Artificial Intelligence. 4

API Application Programming Interface. 4

IT Information Technology. 4

Q-ICT Quality ICT. 4

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.

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**: implementing tools and processes for continuous monitoring of clients' systems, devices, networks, and systems to detect and respond to security threats in real-time.
- **Vulnerability Assessment**: conducting regular vulnerability assessments and penetration testing to identify weaknesses in clients' systems and infrastructure
- **Incident Response**:

The company currently manages numerous third-party APIs for the above-mentioned purposes. Those APIs are the following:

•

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.

1.2 Q-ICT Software Development Department

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:

1.3 Project Objectives

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

1.

2. Develop a

1.4 Reading Guide

Chapter 2

Research Results

„„

2.1 Research Methodology

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)