GRADUATION PROJECT DESCRIPTION

Attention: This form must be returned, via email, to the graduation agency (graduation.ict-ct-emmen@nhlstenden.com).

Explanation:

- The size of the graduation project description must be 1-2 A4 and must contain the points mentioned here below. The format of the fields is not fixed and can be resized to fit.
- It must be clear why this graduation project is of sufficient level (think about the complexity).
- The research should serve the realisation (See phase 2 SDLC.)

Name of student:

Student: Christopher Sulistiyo (4850025)

Institution/company where assignment will be carried out:

Name:	Quality ICT (Q-ICT)
Address:	Kapitein Nemostraat 20
Town, post code:	Emmen, 7821 AC
Department:	Software development
Telephone:	0591 – 708 004
Name of supervisor:	Manuel Weidijk, Mark Kolk
E-mail of supervisor:	manuel@qict.nl, m.kolk@qict.nl
Number of permanent employees:	20

Does the company meet the requirements mentioned in the handbook graduation:

(Think about the requirement about company and placement supervisor.)

Both supervisors are master graduates from the field of IT, with the latter has been working on the field of IT and security department for more than 20 years. Additionally, the company will facilitate the interns with the required resources for an adequate working facility such as work laptop and docking station for a proper desktop environment. The company itself is a cybersecurity company, solely dedicated for security advisor and client-made software development and has received many IT interns from NHL Stenden who got their projects approved before working for the company. Moreover, the company will grant the intern access to essential APIs and platforms (such as SentinelOne, N-Central, and Bodyguard.io) required for the monitoring application, alongside a range of GCP (Google Cloud Platform) services encompassing Google Secret Manager, Firebase, Cloud Functions, Firestore, Google Authentication, Cloud Messaging, Cloud Storage, Google Analytics, hosting services, real-time databases, etc. Additionally, access will be provided to a SCRUM board, as well as both test and live environments essential for software development.

Are the required competencies achieved:

(See graduation project manual, appendix E.)

During this project, the intern will analyze company's existing internal application, identify, and offer advice for any security weaknesses and/or bugs, strategize a design aligning with the project's

objectives and scopes for the company's internal application, and endeavor to implement the planned design within the project duration. The intern will be subjected to a comprehensive learning experience encompassing the creation of process documentation such as monthly reports, thesis, and user manual. Moreover, the intern will gain practical exposure to a real work environment focused on ICT and cybersecurity, engaging in SCRUM management, software development, and receiving guidance from the company supervisor throughout the project duration. This alone should prove that the project has received the final qualifications required to achieve a bachelor's degree in the field of Information and Communication Technology in NHL Stenden.

Furthermore, this project endeavors to alleviate QICT's current challenge of disparate and unstandardized API monitoring within its internal application.

Introduction graduation project:

(Think about the context.)

Q-ICT is a cyber-security consultant company, currently manages numerous third-party APIs without a standardized implementation within its internal applicaton, the QaaS app. The company seeks to establish 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. Those APIs that the company uses on its internal application include:

- Snelstart: is used for company's automation of financial and accounting sytem software, such as managing invoices, etc,. The file returned by this API is in the form of JSON format.
- 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. The file received from this API calls will be in the form of SOAP XML format
- Pax8: is used for their Microsoft subscription. It is a software that helps Q-ICT to simplifiy the way to buy, sell, and manage cloud solutions. The response file returned by this API is in the form of JSON format.
- 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, The file received from this API is in JSON format.
- 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. The file format returned by this API is in the form of SOAP XML.

Project Scope

The project's focus involves enhancing on the QaaS internal app to serve as a versatile template application capable of executingh the aforementioned functionalities. In addition, the company aims to integrate SentinelOne to the QaaS app, a cybersecurity platform yet to be explored by the company. This platform facilititates continuous monitoring the clients' IT environments for any potential cyber threats, utilizing AI tool to analyze endpoint activities in real-time. Upon successful integration without disruption of existing API calls, the company futher desires insights into cyber threats detected by

SentinelOne from its clients' IT infrastructure. These insights, visualized through graphs and charts connecting the API-sourced data, necessitate QaaS app's ability to interpret SOAP XML and JSON file formats. This will then require the intern to create additional front-end pages in Flutter within the internal app to visualize the SentinelOne integration. Moreover, the company expresses its desires to new ideas, including implementing reading capabilities from YAML, TOML, and CSV file format.

Additionally, the company desires the QaaS app to incorporate error logging functionality. This entails the app being capable of listing and exhibiting all the unsuccessful API calls, displaying their respective status codes and messages. It would be also advantageous that the internal app to be able to conduct testing and debugging to these unsuccessful API calls to diagnose issues such as expired credentials, while also being able to inspect the payload for further analysis.

Voluntarily, at the company discretion and if the project duration permits, they desire that the intern to address potential data integrity issues arising from N-Central API calls, which frequently result in errors of the return data.

Consequently, the intern will undertake research to identify and implement optional practices for integrating API monitoring functionalities into an existing application. The internal app, built in Flutter front-end client with a Node.Js TypeScript as the back end server, already encompases functionalities from GCP (Google Cloud Platform) services like Google Secret Manager, Firebase, Cloud Functions, Firestore, Google Authentication, Cloud Messaging, Cloud Storage, Google Analytics, hosting, real-time database, etc,. Additionally, the intern will have access to both test and live environment for DevOps purposes to facilitate continuous integration. Comprehensive unit testing and meticulous documentation are integral components of this project's requirements.

Description research:

(For example, based on a main question and 3-5 sub-questions research must serve the realization. Clearly describe why it's research.

***When approving the assignment, we do not make substantive statements about the main and sub questions. So, keep in mind that these still must be adjusted during graduation and that the main and sub questions in this description are a first step towards**.)*

The following will describe the main research topic question and sub-question that the intern currently has in mind for his graduation project. These main and sub-questions of course can be later a subject to change after a proper consultation with his school lecturers.

The main 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 sub-questions are as follows:

- 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 Sentinel One can be integrated into the Q-ICT environment, specifically aligning with the API monitoring functionality, while still utilizing their 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 application in XML and JSON formats that ensure clear and insightful representation of threats detected by SentinelOne and other Q-ICT relevant API connections?
- What is the industry-standard best practices for developing and implementing a standardized API monitoring functionality on top of an existing internal application with measurements for scalability, security, and reliability insurance of the monitoring application?
- What potential impact can the implementation of the proposed solution have on Q-ICT's operational efficiency, cybersecurity posture, and end-users' perception and interaction with the already existing internal application?

Furthermore, the intern plans to utilizing LaTeX Overleaf as his choice of software system for document preparation. Engaging in this research alone presents the intern with a novel and captivating exploration of a complex IT topic, one that he has yet to delve into previously.

Description realization:

(What the student delivers.)

The project's realization phase will involve the creation of multiple software deliverables, primarily encompassing a Flutter-based client front-end application and a Node.Js Express TypeScript-template based back-end server application as they were pre-determined by the client to ensure their continuous development. These will incorporate a middleware and functionalities source from GCP (such as Firebase, Google Secret Manager, Cloud Functions, Firestore, Google Authentication, Cloud Messaging, Cloud Storage, Google Analytics, hosting, real-time database, etc.,) as well as Q-CT internal third-party APIs mentioned above. The access to the internal APIs will firstly be 2 APIs, N-Central and Bodyguard.io, both returning file format of SOAP XML and JSON respectively.

To provide additional background for the explanation, the company is currently encountering issues with executing API calls on their Firebase Cloud Functions, which have a one-hour limitation on execution duration. Occasionally, when retrieving specific data (such as a particular customer's data), an API calls surpasses this time limit. This problem primarily occurs within Pax8, Snelstart, N-Central, and the company foresees a potential occurrence with Bodyguard.io as well in the future. Therefore alternatively, the intern has been tasked with finding a solution to resolve this issue for at least 2 of the internal APIs, collaborating well with his company supervisor.

This also tackles an additional concern, namely the necessity for multiple API calls to obtain a desired single set of data. The company is then open to any solution that addresses this matter, prompting the intern to devise a method that executes a single function within the internal application. This function would need to work autonomously and asynchronously to handle the required additional API calls,

thereby reducing the time spent on manually calling these APIs on the screen. A resolution to this issue would align effectively with the previously mentioned concern.

This project will also implement proper unit testing, code commenting, code refactoring, with proper design and architectural patterns for scaling and proper UI/UX implementation to ensure ease-of-use for users. Furthermore, the intern and his supervisor will be working in SCRUM Agile methodology with their own SCRUM board containing definition of done, product backlogs, sprint backlogs, burndown chart, etc. The intern and his supervisor will also have their daily stand-ups, sprint review, sprint retrospective, and sprint planning concurrently.

Description of complexity:

(What makes it that this assignment is suitable as a graduation assignment so that the student can achieve the final competences here.)

The complexity of this project lies in the integration of SentinelOne into the already existing QaaS internal application to work well with other APIs utilizing multiple technologies (Flutter, Node.Js, and GCP services), which is a novel undertaking for the company. While throughout the project duration the intern will be in direct contact and guidance from the company supervisor; however, both the company and the intern will navigate to new programming activities. Challenges in this project include establishing a robust security protocol as it handles with a crucial confidential data for the company from the internal APIs, designing intuitive UI/UX with effective visualization, and making an informed decision regarding software design and architectural patterns for continuous integration, database environment, API key management, unit testing strategies, integration approach, deployment and DevOps practices, technology (frameworks, libraries, and tools) selection, adaptation to changes, and security measures.

In conclusion, a well-managed work period of 90-100 days should be deemed adequate for this project, considering the proper distribution and management workflow. The project's complexity aligns with the expectations set by the Bachelor of Information and Communication Technology program at a University of Applied Science.

Date completed: 8-December-2023