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.)

The supervisor is a master-graduate from the field of IT that has been working on the software development department for more than 5 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.)

By doing this project, 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 makes the intern think 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, which is a cyber-security consultant company currently has a lot of third-party APIs and currently do not have a standard on how to implement it in the internal application (QaaS app). The company is looking for a way to monitor those internal APIs, check if connections are being made, check for error, handling API keys to check if they are expired, and looking for more insight from external party if the connections are properly connected to each other. The project is to continue working on the QaaS internal app and make it to be template where those functionalities can be executed.

Additionally, the company also wants to implement either SentinelOne and/or N-Central and Bodyguard.io platforms which both have not yet been looked and researched at by the company. Both are cyber-security platforms used to help continuous monitoring the clients' IT environment for any potential cyber threats. SentinelOne uses AI to continuously monitor and analyze endpoint activities to identify potential threats in real-time. N-Central itself 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. Bodyguard.io itself 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. Furthermore, they want to see how many threats detected with SentinelOne, with a visualization like graphs and charts that connect the data sent by the API, which means the application should be able to read XML and JSON files.

The intern additionally should research what are the best practices for building that API monitoring app as well as the maintenance. The internal app is made in Flutter with the back end of NodeJs TypeScript implementing already existing functionalities from GCP (Google Cloud Platform) like Google Secret Manager, Firebase, Cloud Functions, Firestore, Google Authentication, Cloud Messaging, Cloud Storage, Google Analytics, hosting, real-time database, etc,. The intern will be given both test and live environment for DevOps for continuous integration. A proper unit testing and documentation is also required as of this project.

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 and/or N-Central and Bodyguard.io security threat platforms 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 and/or N-Central and Bodyguard.io platform(s) 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, N-Central, Bodyguard.io, and other relevant API connections?
- What is the industry-standard best practices for developing and maintaining an API monitoring 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?

The thesis itself will adhere to the guidelines provided by NHL Stenden from its module-books and guidance from lecturers. Furthermore, the intern will utilize 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 they have 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 and platforms such as SentinelOne, N-Central, and Bodyguard.io.

This project will also implement proper unit testing, code commenting, code refactoring, with proper design and architectural patterns for scaling and proper user interface 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, 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, N-Central, and Bodyguard.io to the already existing QaaS internal application 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 including 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, the intern thinks that 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 an University of Applied Science.

Date completed: 7-December-2023