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

Listings

Glossary

API is a software intermediary that allows two applications to talk to each other. In other words, an API is the messenger that delivers request to the provider that was requested from and then delivers the response back (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.-e) . 10

REST is a software architectural style for providing standards between computer systems on the web, making it easier to communicate with each other. It is often characterized by how they are stateless and separate the concerns of client and server. (Wikipedia, n.d.-b) . 20

RMM is a software platfomr that helps MSPs remotely monitor and manage their clients' endpoints, networks, and computers (Wikipedia, n.d.-f).. 22

Acronyms

2FA Two-Factor Authentication. 14

A.K.A. Also Known As. 6, 22
ACID Atomicity, Consistency, Isolation, Durability. 17
AI Artificial Intelligence. 9, 22–24
APA American Psychological Association. 11
API Application Programming Interface. 6, 9, 11–16, 18–22, 24
ARP Address Resolution Protocol. 23
AV Anti-Virus. 22, 23
AWS Amazon Web Services. 24, 25

B.V. Besloten Vennootschap. 0, 9, 12
B2B Business-to-Business. 20
BaaS Back-end as a Service. 14

CDR Content Disarm and Reconstruction. 22
CISO Chief Information Security Officer. 10
CMEK Customer-Managed Encryption Keys. 16
CPU Central Processing Unit. 18
CQL Cassandra Query Language. 17
CSF Cybersecurity Framework. 9
CSS Cascading Style Sheets. 15
CT Creative Technology. 0

DB Database. 16–18, 22
DOM Document Object Model. 15

e.g., exempli gratia. 23, 25
ECMA European Computer Manufacturers Association. 15, 16
EDR Endpoint Detection and Response. 11, 22, 23
ERP Enterprise Resource Planning. 14
ES ECMAScript. 16
etc., et cetera. 14, 20, 22, 23
ETDR Endpoint Threat Detection and Response. 22

FCM Firebase Cloud Messaging. 15

FIPS Federal Information Processing Standards. 9

GB Gigabyte. 15

GCP Google Cloud Platform. 14, 16, 17, 24, 25

HTML HyperText Markup Language. 15, 19

HTTP Hypertext Transfer Protocol. 14, 15, 18, 20–22

HTTPS Hypertext Transfer Protocol Secure. 14

IAM Identity and Access Management. 17

ICT Information and Communication Technology. 0, 12, 14

ID Identifier. 24, 25

IoT Internet of Things. 22, 23

IP Internet Protocol. 21

ISO International Organization for Standardization. 10

IT Information Technology. 9, 10, 12, 22, 23

ITIL Information Technology Infrastructure Library. 10

JS JavaScript. 14–16

JSON JavaScript Object Notation. 12, 13, 17, 18, 22

MCDA Multi-Criteria Decision Analysis. 13

MDR Managed Detection and Response. 23, 25

ML Machine Learning. 15, 23

MS Microsoft. 9, 10, 18, 22

MSP Managed Service Provider. 6, 22

N/A Not Applicable. 24

NDR Network Detection and Response. 23

NIST National Institute of Standards and Technology. 9, 10

NoSQL Not Only SQL. 4, 14, 17, 18

OAS OpenAPI Specification. 19

OAuth Open Authorization. 16

OCI Oracle Cloud Infrastructure. 24

OOP Object-Oriented Programming. 15, 16

OS Operating System. 14, 15, 24

OTP One Time Password. 14

Pentest Penetration Testing. 6, 10

PUA Potentially Unwanted Application. 24

Q-ICT Quality ICT. 0, 9–14, 16, 22

QaaS Quality as a Service. 11–16, 20, 22

QL Query Language. 18, 22

RAM Random Access Memory. 15, 18

RDMS Relational Database Management System. 17

REST Representational State Transfer. 6, 20–22

RMM Remote Monitoring and Management. 6, 22

SaaS Software as a Service. 14

SEM Security Event Management. 23

SIEM Security Information and Event Management. 10, 23

SIM Security Information Management. 23

SME Small and Medium-sized Enterprises. 9, 22

SOAP Simple Object Access Protocol. 20–22

SOAR Security Orchestration, Automation, and Response. 23

SOC Security Operations Center. 23, 25

SQL Structured Query Language. 4, 17, 18

SWOT Strengths, Weaknesses, Opportunities, and Threats. 13

TS TypeScript. 14, 16

UI User Interface. 14, 16

URI Uniform Resource Identifier. 20, 21

URL Uniform Resource Locator. 21

UUID Universally Unique Identifier. 25

UX User Experience. 15

vCPU Virtual Central Processing Unit. 15

vs. versus. 4, 18

XML Extensible Markup Language. 12, 13, 17, 19, 20, 22

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.

SentinelOne....

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.

Furthermore, the company also serves as a MS provider....

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 act 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, CISOs, and cybersecurity specialists.
3. *Software Development Department*: it addresses Q-ICT clients' need 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 MS 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, Thus, the company has tasked the author with the development of the SentinelOne security threat platform integration 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. Effectively integrates and leverages the SentinelOne EDR platform for continuous cybersecurity monitoring within the QaaS app.
2. The QaaS app should have a way to visualize the data retrieved from the SentinelOne API in a user-friendly manner in order for the client users helpdesk support, financial department, cybersecurity department, software development department, and other employees within Q-ICT departments to see the data easier.
3. Combine the SentinelOne data with N-Central API
4. Utilize Vigilance package of SentinelOne
5. Ensure proper unit testing, code refactoring, commenting, and adherence to the overall code conventional guidelines and best practices in both the test and live environments of 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 of 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 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 Quality ICT B.V. effectively integrate and leverage SentinelOne EDR platform for continuous cybersecurity monitoring?"

The research sub-questions are then used to function as a pathway that dissects 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 Quality ICT B.V.?
- How can SentinelOne be integrated into the QaaS app environment, 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 other Security Threat Platforms to ensure clear and insightful representation of threats detected by SentinelOne API?
- How should the QaaS app respond in the event of a cybersecurity incident detected through the utilization of SentinelOne technologies and packages?

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: desk research of Literature Study will be conducted, with the goal of creating infrastructure information that displays the structure of the QaaS app and all of its dependencies. Furthermore, Interview with key stakeholders involved in the development, maintenance, and usage of the QaaS app will be conducted to gain insights into the current situation of the app.
- Sub-question #2: Literature Study on various articles on the Internet, interviews, expert reviews, and requirement elicitation techniques such as use case analysis and user stories. Analysis on the current QaaS app and its API monitoring capabilities.
- Sub-question #3: technical evaluations of SentinelOne's capabilities and APIs will be conducted, the API documentation and integration guideline will be read and review with Literature Study method and case studies of similar integrations. Requirements from the cybersecurity experts from the Q-ICT department responsible for SentinelOne's technical support will be gathered and analyzed. Furthermore, Prototyping with proof-of-concept prototypes on a test environment will be conducted to test different integration scenarios, assess feasibility, identify potential challenges, refine the approach, and evaluate the performance of the integration.
- Sub-question #4: research into existing visualization techniques for XML and JSON data, especially the data coming from SentinelOne API through Literature Study. Analyze existing data visualization tools

and platforms that are available in Flutter and Firebase. Gather requirements from project stakeholders regarding data visualization preferences and usability, and do data analysis and usability testing.

2.2.2 Selected Measuring Instruments

- Sub-question #1: structured interview guide, document report checklist analysis and review, observation, analysis tools for codebase and logs, and quite possibly supplemented by surveys or questionnaires.

- Sub-question #2: document analysis tools for literature review. Structured questionnaires for requirement interviews regarding functionality rating scale and compare the response against industry standards and best practices. Observation of existing API monitoring tools. Prioritize functionalities based on importance, feasibility, and impact on the QaaS app.

- Sub-question #3: technical assessments and requirement workshops will be conducted. Furthermore, API documentation review, document analysis tools, security impact risk assessment, and feasibility checklist assessment with the Company Supervisor will also be overseen.

- Sub-question #4: the selected measuring instruments for this sub-question will be through observation of existing data visualization tools, literature review through reading the studies of the best visualization suitability matrix techniques, structured questionnaires to end-user interviews, and usability testing heuristics.

2.2.3 Method of Data Analysis

- Sub-question #1: a qualitative thematic SWOT analysis of interview transcripts and documentation for operational insights to identify strengths, weaknesses, and areas for improvement in the current situation of the QaaS app.

- Sub-question #2: comparative analyze survey/interview responses using MCDA and compare against industry standards and best practices. Prioritize functionalities based on importance, feasibility, and impact on the QaaS app.

- Sub-question #3: evaluate the technical feasibility, compactibility, and alignment of SentinelOne's features with the QaaS app environment. Analyze potential integration challenges and mitigation strategies, and assess the performance of the integration through prototyping and testing. Technical analysis for the API documentation and thematic analysis for interview data.

- Sub-question #4: technical tool analysis by reviewing and evaluating the suitability of different visualization techniques for representing the data processed and received by the QaaS app in XML and JSON formats from the API considering factors such as clarity, interpretability, and user engagement. Do a user-centered design and cognitive load analysis by analyzing feedback from company stakeholders, supervisor, and end-users.

2.2.4 Reliability, Validity, and General Applicability

- Sub-question #1: the reliability of the data can be ensured by triangulation of data from multiple sources and conducting interviews with stakeholders from different departments with structure questionnaires to ensure that the data is consistent and accurate. The validity of the data will be ensured by cross-referencing with the existing literature or industry best practices or other sources and through information obtained from interviews with the QaaS app developers to ensure that the data is accurate and reliable. The general applicability of the data will be ensured by ensuring that the information obtained is relevant and applicable to the research question and that it can be used to draw meaningful conclusions and make informed decisions, furthermore by comparing findings with industry standards and best practices or similar case studies or projects.

- Sub-question #2: ensure reliability through sampling techniques and representative stakeholder involvement, with comprehensive literature review and multiple sources of information. Validate priorities against real-world scenarios or case studies involving diverse expert panel, like the Company Supervisor. General applicability can be assessed by comparing prioritization with similar projects or frameworks, and considering scalability and adaptability of the integration with representative user samples.

- Sub-question #3: the validity of this sub-question will be through pilot integration unit testing or proof of concept documents, and ensuring alignment with cybersecurity standards and best practices. The reliability will be to consider future needs such as adaptability and scalability of the integration, and focus on Q-ICT user context and needs. General applicability can be assessed by comparing integration strategies with industry standards or expert opinions such as from the Company Supervisor.

- Sub-question #4: reliability can be defined by ensuring future adaptability with comprehensive literature review and multiple sources of information. Validity can be achieved through validating visualization choices through data-driven approach in usability testing or prototyping, ensuring alignment with best practices in data visualization and involving the expert, like the Company Supervisor on the field. General applicability can be assessed by accessibility

considerations by comparing proposed visualization techniques with similar applications or domains.

2.2.5 Research Limitations

The project and research in general will be limited on the API request methods, in which the author is allowed to do only GET requests. This is due to the fact that the author is not allowed to do any PATCH, POST, PUT, DELETE, or any other HTTP request methods that could potentially change the state of the QaaS app or the API that is being requested. This limitation is because the author is not a full-time employee of Q-ICT and is not allowed to make any changes to the QaaS app or the API that is being requested. Therefore, the author is limited to do research in the best practices and possible answer for API monitoring and integration for the GET request method only.

The author is also limited in showing the SentinelOne dashboard

Moreover, the author is also limited to the non-disclosure agreement signed within the initialization period of the graduation work placement. This means that any confidential information that the company deems as confidential will not be disclosed in this research. This includes any information that is not publicly available, such as any financial data or security data pertaining to the internal system or the QaaS app internal code.

2.3 Research Sub-Question #1

The QaaS app is an ERP web application that is used by Q-ICT and its clients. For Q-ICT's clients, it is a SaaS that is used.... For Q-ICT itself, it is an ERP system that is used to manage the clients and their ICT infrastructure. It is made in Dart with Flutter as the front-end framework. There are 2 main parts of the QaaS app, the front-end and the back-end. The front-end is made in Flutter, and the back-end is made in Node.js with TypeScript as the template. The back-end is hosted on Firebase Cloud Functions which are used to connect and make HTTP calls to the internal APIs, and the front-end is hosted on Firebase Hosting.

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.-d).

Cloud Solutions

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 (Wikipedia, n.d.-c).

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. The services offered by Firebase including (Firebase, n.d.)

- Databases:
  - 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.
  - Real-time database:
- Authentication: is an easy-to-understand authentication services that support various authentication methods like email/password, phone number, with identity providers such as Google, Facebook, Twitter, Apple, GitHub, etc., along with utilizing 2FA authentication factors to enhance security by requiring additional factor, such as an OTP code that is sent to the user's phone or security key.
- Cloud Functions: often just called Functions in the Firebase console, it allows developers to run back-end code in response to events triggered by Firebase features and HTTPS requests. The code is stored in Google's cloud and runs in a managed environment. It is a serverless framework that allows developers to build and deploy serverless functions that automatically scale up and down based on demand. The available programming languages are Node.js (JS and TS), Python, Go, Java, and .NET (C#). Cloud Functions offers 2 product versions: the original version (1st gen), and the 2nd gen which is built on Cloud Run and Eventarc to provide an enhanced feature set.
  - 1st Generation: Most of the Firebase Cloud Functions that are used in the QaaS app are in this version. The company wishes to migrate all the functions to the 2nd generation in the future.
  - 2nd Generation: The company wishes that the author's graduation project will utilize the 2nd generation of Cloud Functions. Features in the 2nd generation including:

* Longer request processing times
* Larger instance sizes
* Traffic management
* Eventarc integration
* Broader CloudEvents support

Feature	1st Gen	2nd Gen
Image registry	Container Registry or Artifact Registry	Artifact Registry only
Request timeout	Up to 9 minutes	• Up to 60 minutes for HTTP-triggered functions • Up to 9 minutes for event-triggered functions
Instance Size	Up to 8GB RAM with 2 vvCPU	Up to 16GB RAM with 4 vCPU
Concurrency	1 concurrent request per functions instance	Up to 1000 concurrent requests per function instance

Table 2.1: Comparison between the 1st and 2nd Generation of Cloud Functions

- Hosting: a service that allows developers to host static websites, dynamic web apps, mobile apps, and microservices on Firebase's infrastructure. The QaaS app is currently hosted on Firebase Hosting.
- Cloud Messaging/FCM: allows developers to send push notification and targeted messages to a client app that new email or other data is available to sync, or send notification messages to drive app interaction, adding more user re-engagement and retention. It is a cross-platform messaging solution that lets developers reliably deliver messages at no cost.
- Cloud Storage: offers a secure, scalable, and reliable file storage and sharing for Firebase apps. It is designed to help developers quickly and easily store and serve user-generated content, such as photos or videos.
- Remote Config: allows developers to dynamically control and the change behaviour and appearance of their apps without publishing app updates and requiring users to download them.
- Performance Monitoring
- Analytics: provides free and unlimited analytics solutions for understanding app usage, user engagement and user behaviour by tracking event logging, user demographics, and funnel analysis to gain valuable insights to improve the app.
- Crashlytics: is a lightweight, real-time crash and error reporter that helps developers track, prioritize, and fix stability issues that erode to the quality of the developer's app.
- Test Lab: enables automated testing of the developer's app on real devices in the Google data center.
- Dynamic Links: consist of deep links that dynamically route users to the content they are interested in, across platforms and devices. It helps developers create and share links that work the way they want, on the platform they want, and whether users have their apps installed.
- ML Kit: provides a set of ML APIs that can be easily integrated developer's app. This feature is still in beta testing.

JavaScript

JS is a high-level, interpreted programming language that conforms to the ECMAScript specification. It is a multi-paradigm programming language, supporting OOP, imperative, and functional programming styles and is primarily used for client-side web development. It is also used for server-side development with Node.js, and for mobile app development with frameworks like React Native, Vue.js, Angular.js, and NativeScript. JS is now one of the core technologies of the web, along with HTML and CSS, and is supported by all modern web browsers. Some key features of JS include:

- Client-side Scripting: it is mainly used for client-side scripting in web browsers, allowing programmers to create dynamic content that interacts with the browser and the user. It can manipulate the content and behavior of HTML elements, respond to user actions without the need to reload the page for interacting with DOM to update page content dynamically. This enhances the UX by making web applicaitons feel more responsive and integrated.
- Cross-Platform Compactibility: it is supported by all modern web browsers, including Chrome, Firefox, Safari, Opera, and Edge, and can be used to build cross-platform web applications that run on any device or platform, like Android or iOS.
- Server-Side Scripting: with the advent of Node.js,

it has also become popular for server-side scripting. Node.js is a runtime environment that allows developers to build scalable network applications, including web servers, APIs, and real-time applications like chat servers. This has expanded the versatility and use cases of JS beyond the browsers, making it a full-stack development language.

- Dynamic Typing: it means that variables do not have predetermined types. Instead, types are determined at runtime based on the assigned values.
- Functional Programming: it supports concepts such as first-class functions, high-order functions, and closures. This allows programmers to write more concise and expressive code by treating functions as first-class citizens.
- Event-Driven Programming: it follows an event-driven programming paradigm, where actions or events trigger specific functions or code execution, makes it well-suited for building interactive UI and handling user interaction.

Node.js

is an open-source, cross-platform, server-side runtime environment built on Chrome's V8 JS engine that allows programmers to run JS code outside a web browser, enabling the development of server-side and networking applications.

TypeScript

is an open-source programming language developed and maintained by Microsoft. It is a superset of JS, meaning that any valid JS code is also valid in TS. It adds optional static typing to JS, which allows developers to annotate their code with type information, catch errors early in the development, and improve the maintainability or large codebases. Some developers prefer using TS over JS for some of its key-features:

- Static Typing: it checks the types of variables at compile-time, which enable developers to specify the types of variables, functions parameters, and return values. This introduces type safety, in contrast to JS which is dynamically typed, which means that the types of variables are determined at runtime.
- Enums: it provides supports for enums, allowing developers to define a set of named constants with associated values.
- Generics: it supports generics, enabling the creation of reusable components that can work with a variety of data types.
- Decorators: it supports decorators, which are a way to add annotations and a meta-programming syntax for class declarations and members. Decorators can be used to modify classes, methods, and properties at design time, providing a powerful way to extend or modify the behaviour of classes and their members.
- Interfaces and Classes: it supports OOP concepts such as classes, interfaces, inheritance, and access modifiers, making it easier to organize and structure code.
- ES6+ Features: it supports many features introduced in ECMAScript standards beyond ES5, such as arrow functions, classes, async/await syntax, and modules.
- Backwards Compactibility: it is designed to be backwards compactible with JS, which means that developers can use it alongside JS code and integrate it into existing JS projects and environments, including, browsers, Node.js, and other JS runtime environments.

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.

Secret Manager

It is a fully managed service provided by GCP that allows developers and organization to securely store, access, and manage sensitive information such as API keys, passwords, certificates, OAuth credentials, DB credentials and other credentials used in throughout the lifecycle of their applications (Google, n.d.). It is not part of Firebase, and it helps the QaaS app to centralize and secure its secrets in scalable and easily manageable way. Key-features of Secret Manager include:

- Secure Storage: it encrypts the secret values using CMEK, ensuring the sensitive data is protected both at rest and in transit.
- Audit Logs: it provides and manages audit logs that record all access and modification of activities, helping developers meet compliance, better accountability and regulatory requirements.
- Versioning and Automatic Rotation: it supports versioning of secrets, allowing developers to store multiple versions of the same secret. This means that the

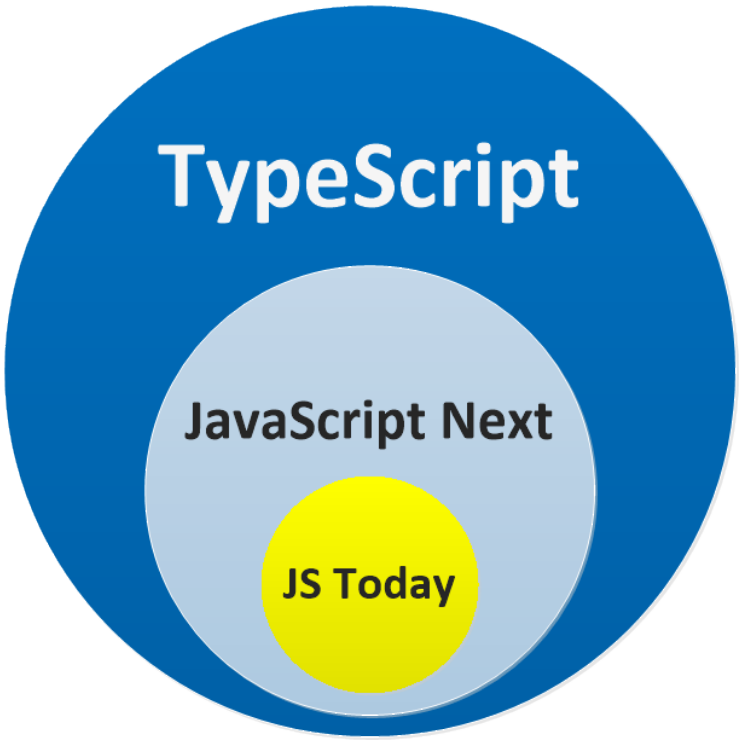

Figure 2.1: Venn diagram of TypeScript and JavaScript

developers get to keep multiple versions of secrets and easily revert or roll back to a previous version if needed, which will help in auditing and tracking changes to secrets over time. This feature enables automatic seamless rotation of secrets at regular intervals without disrupting the applications, which improves the security part of the application by ensuring that secrets are regularly updated without manual intervention.

- Access Control: it provides fine-grained access control using Google IAM, allowing developers to specify who can access and manage the stored secrets and what they can do with them.
- Centralized Management: it stores and manages all secrets in one place, simplifying access and control.

Cloud Functions can typically access GCP Secret Manager by....

NoSQL Database

is a category of DB that provides a mechanism for storage and retrieval of data that is modelled in ways other than the tabular relations used in RDMS. NoSQL DBs are typically designed to handle large volumes of unstructured or semi-structured data, such as JSON, XML, or binary objects, and they offer a flexible data model that can evolve over time. Both databases in Firebase, Firestore, and Real-time Database are NoSQL databases. Some characteristics of NoSQL DBs include (MongoDB, n.d.):

- Data Model: NoSQL uses dynamic schema, which allows data to be inserted without having to define the schema first, while SQL uses a fixed schema to store data.
- Data Structure: NoSQL DBs use a variety of data structures such as key-value pairs, document-oriented, graphs databases, and columns-oriented; unlike SQL which only uses tables to store data.
- Querying: NoSQL uses variety of query languages, such as MongoDB query language or Cassandra's CQL, while SQL databases only use SQL as the unified language to query data.
- Data Consistency and ACID Compliance: databases that are ACID compliant means that they follow a set of rules to ensure that database transactions are processed reliably and securely. SQL databases are a good example of this, while NoSQL databases sacrifice some ACID properties in order to achieve higher performance and scalability.
- Use Case: NoSQL DBs are ideal for applications that need to handle large volumes of data and require high scalability and flexibility, such as social media platforms, real-time analytics, and content management systems.
- Scalability: NoSQL databases are traditionally designed for horizontal scalability, meaning they can easily scale out multiple servers or clusters to handle volumes of data and high throughput, which is more cost-effective and allows for better scalability. They are well-suited for distributed and cloud-based

environments. SQL databases are traditionally designed for vertical scalability, meaning a single server is scaled up with more powerful hardware and power (CPU, RAM) to a single server. This can become expensive and limit scalability.

”Serverless Architecture”

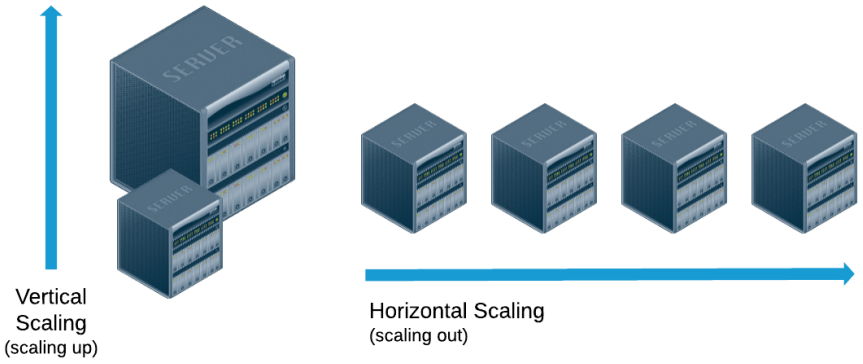

Figure 2.2: Vertical (SQL) vs. Horizontal (NoSQL) Scaling

Some examples of NoSQL databases include MongoDB (document-oriented), Cassandra (wide-column store), Redis (key-value store), and Neo4j (graph database). Some examples of SQL databases include MySQL, PostgresQL, and MS SQL Server.

2.3.2 Q-ICT Internal APIs

What is an API?

API is a software intermediary that allows two applications to talk to each other. They are an accessible way to extract and share data within and across organizations.

Web APIs

A web API is an API that can be accessed using the HTTP protocol. Not all APIs are web APIs; some APIs are used only to communicate between two applications on the same computer, never making use of a web connection. But in practice, when developers talk about APIs, they are almost always talking about web-based APIs used to

JSON format JSON is a lightweight data-interchange format that is easy for humans to read and write while being also easy for machines to parse and generate too. It is based on a subset of the JavaScript programming language and is commonly used for representing structured data. JSON is often used for transmitting data between a server and a web application, as well as for storing configuration data.

JSON data is organized into key-value pairs, where keys are strings and value can be strings (enclosed in double quotes ‘””‘), booleans (‘true‘ or ‘false‘), numbers, objects (unordered collections of key-value pairs enclosed in curly braces ”), arrays (ordered collections of values enclosed in square brackets ’[]’), or null.

Listing 2.1: Example of a JSON response

```
{
    "name": "John Doe",
    "age": 30,
    "isStudent": false,
    "cars": [
        {"name": "Ford", "models": ["Fiesta", "Focus", "Mustang"] },
        {"name": "BMW", "models": ["320", "X3", "X5"] },
        {"name": "Fiat", "models": ["500", "Panda"] }
    ],
    "hobbies": ["Reading", "Gaming", "Traveling", "Cooking", "Photography",
        "Painting", "Gardening"],
    "address": {
        "street": "Sesame Main Street",
```

```
            "city": "New York",
            "zip": "10001"
        }
    }
```

XML format XML is a markup language that defines a set of rules for encoding documents in a format that is both human and machine-readable. It provides a way to structure data in a hierarchical format using tags to define elements and attributes within those elements. It is often used for store, design, and representing structured data in a portable and platform-independent way, making it easy to create, exchange, and process information between different systems, applications, and platforms.

XML documents consist of text-based data enclosed in tags, similar to HTML, but allows users to define their own customized tags and document structures. This flexibility makes XML suitable for representing a wide variety of data types and structures.

XML is often used in various domains such as web services, configuration files, data interchange between different software systems, and more.

Listing 2.2: Example of a XML response

```
<response>
    <status>200</status>
    <message>OK</message>
    <data>
        <user>
            <id>123</id>
            <username>johndoe</username>
            <email>johndoe@example.com</email>
            <role>user</role>
        </user>
        <user>
            <id>456</id>
            <username>janedoe</username>
            <email>janedoe@example.com</email>
            <role>admin</role>
        </user>
    </data>
</response>
```

OpenAPI Standard Previously known as Swagger, OAS is a specification for writing a public API, with guidelines for details like endpoint naming conventions, data formats, and error messaging (Swagger, n.d.). The standards required by OpenAPI and its automation of some tasks make it easier for a developer to start working with an API without needing to read through a complex code base. For API producers, OpenAPI standard offers access to a wide variety of tools based on the standards. API teams can use these tools to quickly up mock servers and create high-quality documentation, among other tasks. APIs are generally categorized into different types based on their audience, architecture, and protocols (Bahl, 2022):

Different Types of API By Audience

Public API: also called external or Open API, and as the name suggests it is available to everyone. They are open for the public to use and integrate with their applications. Developers can quickly implement them using little to no authorization, with few require sign-up and generation of the API Keys to access them. This can make them to not be the best regarding security - just because ”public” means expanded visibility - but sharing data with them is easier.

Examples of a public API are OpenWeatherMap, Google Maps navigation, Facebook and the Twitter API, which the latter allows developers to access Twitter’s functionality and data.

Internal API: also called Private API, and is used within a private organization to make internal apps ”talk” to each other. To interact with the data, a developer needs to be actively granted permission to access it, because the data and functionality available through the API are proprietary to the company. They are often set up with extensive logging and load-balancing capabilities because they must have greater fault tolerance and security than public APIs. They also do not follow the OpenAPI standard as consistently as public APIs, since their producers and consumers typically work together closely, data formats can be negotiated based on specific use cases. As they are built by specifically the

company; it will only have API protocol types that the organization wants to support. All the APIs managed by the QaaS app fall into this category. This solution tend to be very secure, as they are entirely internal.

Partner API: also called Shared API, this API is made considering the scalability while developing the business, which will share a few APIs across a few other licensed organizations, enabling service offerings across business (B2B). This API is shared only with the intended users; others might not have access to them because they are not shared publicly, thus making it exists somewhere between public and private APIs. They often function to share data between two companies or organizations for a specific business purpose, while still ensuring strict privacy protection.

These APIs indeed require authorization to access them (like having a PayPal account or an API key). All the clients who are part of the business can access and integrate using those APIs. Few APIs will only provide read access, and few will provide read/write access via shared APIs. This depends on the business process model.

For example, travel booking APIs are shared with travel agencies to increase their visibility and booking. Websites like Expedia, Make My Trip, and Trivago are excellent examples of this kind of API.

Different Types of API Protocols

SOAP APIs: are strictly based on XML for the message structure and HTTP for the protocols. SOAP itself is a protocol and sending a SOAP request is similar to using an envelope to send a message. SOAP APIs consume extra overhead and more bandwidth, and require more work on both the client and server ends. That being said, like envelopes, SOAP encloses more stringent security compared to REST. XML-encoded SOAP messages use the format defined below:

- **Envelope**: the root element of the message, which encapsulates the entire SOAP message. It 'envelopes' the message by placing tags at the start and the end.
- **Header (optional)**: defines specific additional message requirements, such as authentication.
- **Body**: the request of response is included here.
- **Fault (optional)**: information about errors that might arise during the execution of the API call or response is highlighted here, along with information on how one can address these errors.

Listing 2.3: Example of a SOAP request

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:example="http://example.com">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <example:GetUser>
            <example:UserID>123</example:UserID>
        </example:GetUser>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

REST API: if SOAP is like an envelope, REST is like a more lightweight postcard. REST APIs are considered the gold standard for scalability and are highly compatible with microservice architecture. It is the often used protocol in the context of building APIs for web-based applications. REST itself is not a protocol, but an architectural style for designing networked applications, defining a set of constraints and principles that define how web services should be structured and interact with each other (*see REST*).

APIs that follow REST principles are called RESTful APIs. The are RESTful as long as they comply with the 6 guiding constraints of a RESTful system (Fielding and Taylor, 2000):

- **Client-server architecture**: the architecture is composed of clients, servers, and resources, and it handles requests through HTTP.
- **Statelessness**: no client is stored on the server between requests. The server should process and complete each request independently. Information about the session state is, instead, held with the client. The clients can do this via query parameters, headers, URIs, request body, etc.,
- **Cacheable**: simply, the clients should be able to determine whether this response is cacheable from their side, and if so, for how long. If a response is cacheable, the client has the right to return the data from its cache for an equivalent request and specified period, without sending another request to the server. A well managed caching mechanism can eliminate the need for some client-server interactions
- **Layered system**: client-server interactions can be mediated by additional layers. These layers could offer additional features like load balancing, shared caches, or security.

- **Uniform interface**: this is the core to design RESTful APIs. There should be a uniform and standard way of interacting with a given server for all client types. The uniform interface helps to simplify the overall architecture of the system. This includes 4 facets:
  - Resource identification in request: resources are uniquely identified in requests and are separate from the representations that are returned to the client using URI.
  - Resource manipulation through representations: clients receive files of a uniform that represent resources. These representations must have enough information to allow modification or deletion of the resource's state in the server, as long as they have the required permissions.
  - Self-descriptive messages: each message returned to a client contains enough information to describe how the client should process the information further, such as additional actions that can be performed on the resource.
  - Hypermedia as the engine of application state: after accessing a resource, the REST client should be able to discover through hyperlinks all other actions that are currently available.
- **Code on demand (optional)**: servers can extend the functionality of a client by transferring executable code.

REST APIs are high-performing (especially over HTTP2), time-tested, and support many data formats. They also decouple the client and server, making sure of independent evolution. However, building a true REST API is difficult because it requires a disciplined adherence to the Uniform Interface constraint (Hazaz, 2022). Some organizations trade off the long-term benefits of a truly REST API for other HTTP API protocols that have similar benefits but adhere to REST constraints more liberally. REST requests typically include these key components:

- **Endpoint**: the uniform resource identifier that locates the resource on the internet is part of this component. URLs are the most common type of URI.
- **HTTP Method**: this component outlines the four basic processes that a resource can be subjected to: POST (create a resource), GET (retrieve a resource), PUT (update a resource), and DELETE (remove a resource).
- **Headers**: data related to the server and the client are stored in this component. Like in SOAP, one can also use REST headers to store authentication measures such as API keys, server IP addresses, and the response format.
- **Body**: this component contains additional information for the server, such as data that needs to be added or replaced.

Listing 2.4: Different HTTP methods in REST

```
GET /users Retrieve list of all users
GET /users/{id} Retrieve details a specific user by their ID
POST /users Create a new user
PUT /users/{id} Update a specific user by their ID
DELETE /users/{id} Delete a specific user by their ID
```

Listing 2.5: REST's Example Request

```
GET https://api.example.com/users/123
```

Listing 2.6: Example of REST request in JavaScript

```
const apiUrl = 'https://api.example.com/users/123';

// Define the request parameters
const requestOptions = {
    method: 'GET', // HTTP method (GET, POST, PUT, DELETE, PATCH, etc.)
    headers: {
        'Content-Type': 'application/json', // Set the content type of the request
    }
};

// Make the API request
fetch(apiUrl, requestOptions)
    .then(response => response.json())
    .then(data => console.log(data)) // Process the response data
    .catch(error => console.log('error', error)); // Handle any errors that occurred during the
        request
```

All three of the REST, SOAP, and GraphQL use the HTTP protocol for communication therefore falls into HTTP APIs category. They are the commonly used for web services and allow applications to interact with each other over the internet. HTTP is superbly suited for applications following a request-response paradigm.

With that being said, the QaaS app needs to manage and make connection different sort of APIs. Those APIs are the following:

- Resello: is used for Q-ICT MS 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.
- Bodyguard.io: is a CDR tool 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 RMM 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. The return response from this API is in XML and JSON format, making it both a REST and SOAP API.

2.4 Research Sub-Question #2

2.4.1 SentinelOne

To answer this research sub-question, a general understanding of what SentinelOne is needed in order to know what methods should be utilized to integrate it with the QaaS app.

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.

Some terminology that the readers need to be familiar with before diving deeper into SentinelOne:

Endpoint

Endpoint can be defined as any remote computing devices that receives incoming communications and sends outgoing messages to the network it is connected to. Examples of endpoints include desktops, laptops, smartphones, tablets, servers, workstations, and other IoT devices that is connected to a network. They are the first-line of defence for the Blue team today.

EPP

EDR

EDR A.K.A. ETDR, is a group of integrated endpoint security solutions that combine data collection, data analysis, forensics, and threat hunting with the end-goal of identifying and stopping any potential security breaches in due time. EDR solutions are able to recognize any suspicious patterns that can be investigated later on, as they have been purposefully created to detect and respond in an active manner to advance malware, ransomware, and other cyber threats (the Response EDR). EDR, as the name suggest, were developed specifically for endpoints, and not networks (2.4.1).

The number one thing that sets apart EDR from traditional AV is that traditional AV relies on signature-based detection, usually having a defined set of list in their DB, where known malware signatures are compared against files or processes to identify threats. EDR on the other hand, uses a combination of signature-based detection, such as behavioural analysis, machine learning, and anomaly detection to identify and respond both known and unknown threats. EDR solutions focus on detecting malicious activities at the endpoint level, including file modifications, process execution, and network connections, focusing on malicious behaviour compare to only concerning with malicious software like what traditional AV does.

MDR

NDR

SIEM

is a software system that collects, aggregates, normalizes security data from a variety of sources within an IT

infrastructure, and analyzes it according to pre-set rules, present it in human-readable format and therefore giving a comprehensive picture of the company's information security. SIEM tools evolved from the log management discipline and combine SIM and SEM technologies. A SIEM tool uses AI to automate a number of manual procedures related to threat detection and incident response. Furthermore, it assists enterprise security teams in spotting anomalies in user behavior.

- Input: logs, threat intel, vulnerability feeds, NDR, and EDR data
- Output: high-fidelity alerts prioritized by severity
- Infused with: AI, ML, and analytics

XDR

is a security solution that gathers and analyzes data from multiple sources like endpoints, networks, cloud, emails, app, etc., It offers great visibility into a company's IT infrastructure, helping the security employees to detect more threats, respond efficiently, and deal with fewer false positive alerts Vazquez, 2021.

This solution integrates several tools combining all the gathered data into a single platform to visualize the information. It might incorporate automated processes (even complex ones), ML, and advanced analytics to enable quicker and more effective incident response. It can deal even with hidden and advanced malware.

MXDR

Some people still call it MDR, managed SOC, or managed security.

SOAR

SOAR solutions focus on automating incident response processes and triage capabilities. The main goal is to oversee security without human help as much as possible, boosting productivity and shorten the response time. It might use AI and ML to assess security events and automate incident response procedures. These solutions can be standalone product, or it can be added to SIEM solutions since SOAR does not excel in event analysis.

SOC

Please note that as mentioned before, SIEM can also take data from an EDR and NDR but for the sake of simplicity, the diagram puts them as a separate pier systems.

2.4.2 SentinelOne Console

2.4.3 SentinelOne Agent

An Agent is a software program, deployed to each endpoint, including desktop, laptop, server or virtual environment, and runs autonomously on each device, without reliance on Internet connection, enabling data gathering, detection, and response to actions. Agents can be interpreted as an AV, collecting relevant security telemetry such as:

- Running processes
- Connected servers
- Open files

This information can be useful to detect the presence of a threat or to use in forensic analysis and investigation after an attack has occurred (Recovery).

2.4.4 Ranger

Ranger is one of the SentinelOne product that provides a way of detecting other devices (computers and IoT devices) that are on the client's computer network. If a malicious attacker comes in and plugs his device into the network, all the other SentinelOne agents are going to read the network traffic, determine and classify whether this is a new device, or a rogue device. As long as a device has Ranger on that network subnet, SentinelOne can gather and detect technical information regarding the device. On a network, before a machine is connected and talks to other devices and gateways, it is going to do a broadcast and gives up information about itself. This is called an ARP request. Ranger is going to read that ARP request and determine

2.4.5 Sentinels

Sentinels are the end-points,

2.4.6 Incidents

- Kill: stops all processes related to that threat
- Quarantine: encrypts and moves the threat and its executables
- Remediate: deletes all files and system changes created by the threat
- Rollback: restores files and configuration that the threat changed. This step is usually taken when a malware has executed its script and has made changes to the system, e.g., a ransomware has encrypted all the files and asked for a ransom. By executing this step, all the three previous steps will also be undertaken as well. This will then reboot the system and restore it to the safe state before the malware has executed.

Additionally, the user can also perform an analysis verdict

- False positive
- Suspicious

- True positive
- Undefined

Threat mitigation status

- Mitigated
- Not mitigated
- Marked as benign

Incident status

- Resolved
- Unresolved
- In progress

AI confidence Level

- Malicious
- Suspicious
- N/A

Classification

- Malware
- PUA
- Virus
- Infostealer
- Hacktool

OS

- Windows
- Linux
- Mac
- Windows Legacy

Cloud Provider

- Azure
- AWS
- GCP
- OCI
- ESXI

Engine

- SentinelOne Cloud
- On-Write Static AI - Suspicious
- Behavioral AI
- On-Write Static AI
- Reputation
- Cloud Detection
- User-Defined Blocklist
- Documents, Scripts
- Anti Exploitation / Fileless
- Intrusion Detection
- Potentially unwanted application
- Lateral Movement
- Remote Shell
- Manual
- Application Control
- Threat Intelligence
- WatchTower
- Driver Blocking

Initiated by:

- Agent Policy
- Full Disk Scan
- Local agent command
- Deep Visibility Command
- Management console API
- On-Demand Scan
- Custom Rule
- Custom Alert
- Cloud Detection
- Threat Intelligence
- WatchTower

Additionally, users can also search the mitigated threats by:

- Content Hash
- Cloud Account
- Cloud Image
- Cloud Instance ID
- Cloud Instance Size
- Cloud Location
- Cloud Network
- AWS Role
- AWS Security Groups

- AWS Subnet IDs
- Azure Resource Group
- GCP Service Account
- Threat Details: e.g.,: ”This is a non-Microsoft binary that masquerades as a Microsoft executable”
- File Path: e.g.,: ”\Device\HarddiskVolumeA\Users\Chris\Downloads\malicious.exe”
- Endpoint Name” e.g.,: ”LT-Christopher”, ”LT 10-08”
- UUID: e.g.,: ”0ff2a3409f284776a23432e9f6894afa”
- Agent Version (at detection): e.g.,: ”23.1.4.650”
- Agent Version (current)
- Domain (at detection time)
- Command Line Arguments
- Initiated By (username): e.g.,: ”LuukAdmiraalMKBIT”
- Storyline
- Originated Process
- Cluster Name
- Node Name
- Namespace Name
- Namespace Labels
- Controller Name
- Controller Labels
- Pod Name
- Pod Labels
- Container Name
- Image Name
- Container Labels
- External Ticket ID
- Node Labels

Furthermore, it will also analyze for infected endpoint connectivity (offline/online), mitigated preemptively (yes/no), reboot required (yes/no), action failed (yes/no), pending actions (yes/no), and if note and external ticket exists (yes/no).

2.4.7 Reports

2.4.8 Vigilance

It is a MDR service - providing threat monitoring, hunting, and response, to its existing customers. It provides a 24/7 SOC with expert analysts and researchers to give customers near real-time threat monitoring, in-console threat annotations, and response to threats and suspicious events. Vigilance itself is a separate package from SentinelOne.

2.5 Research Sub-Question #3

Please keep in mind that in this sub-question, only the visualization techniques will be assessed, compared, contrasted, evaluated, and discussed. The other factors such as pricing, technologies, and features will not be discussed in this sub-question.

2.5.1 Heimdal®

2.5.2 Huntress

2.5.3 CrowdStrike

CrowdStrike Falcon

2.5.4 Datto RMM

2.5.5 Sophos

2.5.6 Carbon Black

2.5.7 Trend Micro

Trend Micro Apex One

2.5.8 Kaspersky Endpoint Security

2.5.9 Bitdefender

Bitdefender Gravity Zone

2.5.10 McAfee

2.5.11 Symantec

2.5.12 Trend Micro

2.5.13 Cynet 369

2.5.14 Microsoft Defender for Endpoint

2.6 Research Sub-Question #4

Chapter 3

Realization

Chapter 4

Conclusion and Recommendation

Bibliography

Bahl, J. (2022). Api types and protocols. *Stoplight*. https://stoplight.io/api-types

Fielding, R. T., & Taylor, R. N. (2000). Architectural styles and the design of network-based software architectures. *University of California, Irvine*. https://ics.uci.edu/~fielding/pubs/dissertation/top.htm

Firebase. (n.d.). Firebase products - google. *GCP, Google Cloud Platform*. https://firebase.google.com/products-build

Google. (n.d.). Google cloud. *Secret Manager*. https://cloud.google.com/security/products/secret-manager

Hazaz, Y. (2022). Understanding rest apis: Key principles and best practices explained. *Amplication*. https://amplication.com/blog/rest-apis-what-why-and-how/

MongoDB. (n.d.). What is nosql? *MongoDB.com*. https://www.mongodb.com/nosql-explained

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

Swagger. (n.d.). Openapi specification. *Swagger.io*. https://swagger.io/specification/

Vazquez, M. (2021). What you should consider about extended detection and response (xdr). *IDC*. https://blogs.idc.com/2021/03/18/what-you-should-consider-about-extended-detection-and-response-xdr/

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). Api. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/API

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

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

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

Wikipedia. (n.d.-f). Remote monitoring and management. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Remote_monitoring_and_management

Appendix A

Planning

Appendix B

Project Plan

Appendix C

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