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

List of Tables

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**) . 10

CAPTCHA is a type of challenge-response test used in computing to determine whether or not the user is human (*Wikipedia, n.d.-d*) . 21

CRM is a process or strategy that companies use to manage and analyze customer interactions and data throughout the customer lifecycle. CRM technology is a software system that helps organizations easily track all communications and nurture relationships with their leads and clients *Wikipedia, n.d.-f* . 17

ERP is a type of software that organizations use to manage core day-to-day business activities needed to run a company such as accounting, finance, procurement, project management, manufacuring, risk management and compliance, HR, and supply chain operations (*Wikipedia, n.d.-h*) . 17

NoSQL 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 (*MongoDB, n.d.*). 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. . 20

Pentest A.K.A. ethical hacking, is a simulated cyberattack where professional ethical hackers break into corporate networks to find weaknesses (Wikipedia, n.d.-k) . 15

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 (**IBM, n.d.**) . 23

RMM is a software platfomr that helps MSPs remotely monitor and manage their clients' endpoints, networks, and computers (Wikipedia, n.d.-l). 17

Cron Job is a job scheduler responsible on scheduling tasks on repeated schedule on a server (*Taylor, 2024*) . 21

Network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use ion analysis, security or general network management . 26

reCAPTCHA is a CAPTCHA system owned by Google to enable web hosts to distinguish between human and automated access to websites (*Wikipedia, n.d.-e*) . 21

Threat Hunting A.K.A. cyberthreat hunting, is a proactive approach to identifying previously unknown, or ongoing non-remediated threats, and searching for signs of potential cyber threats within an organization's network or system (*Wikipedia, n.d.-g*) . 26, 28

Acronyms

2FA Two-Factor Authentication. 20, 21

A.K.A. Also Known As. 6, 26, 31
AI Artificial Intelligence. 10, 25, 26, 29
APA American Psychological Association. 11
API Application Programming Interface. 6, 10, 12–14, 16, 17, 20, 22–25, 28–30
ARP Address Resolution Protocol. 28, 29
AV Anti-Virus. 15, 16, 25, 26, 28, 32
AWS Amazon Web Services. 26

B.V. Besloten Vennootschap. 0, 12
B2B Business-to-Business. 23
BaaS Back-end as a Service. 20

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart. 21
CDR Content Disarm and Reconstruction. 17
CISO Chief Information Security Officer. 15
CMEK Customer-Managed Encryption Keys. 22
CRM Customer Relationship Management. 6, 17
CSF Cybersecurity Framework. 14
CT Creative Technology. 0

DB Database. 6, 16, 22, 26
DHCP Dynamic Host Configuration Protocol. 29
DNS Domain Name System. 26

e.g., exempli gratia. 29
EDR Endpoint Detection and Response. 10, 26, 28, 32
EPP Endpoint Protection Platform. 25, 26, 32
ERP Enterprise Resource Planning. 6, 16, 17
etc., et cetera. 16, 20, 24, 26
ETDR Endpoint Threat Detection and Response. 26

FIPS Federal Information Processing Standards. 14

GB Gigabyte. 21

GCP Google Cloud Platform. 20, 22

GUID Global Unique Identifier. 6

HR Human Resources. 6

HTTP Hypertext Transfer Protocol. 13, 17, 20, 21, 23–25

HTTPS Hypertext Transfer Protocol Secure. 20

i.e., id est. 16

IAM Identity and Access Management. 22

ICT Information and Communication Technology. 0, 12, 17

IDS Intrusion Detection System. 26

IoT Internet of Things. 25, 28

IP Internet Protocol. 24, 29

IPS Intrusion Prevention System. 26

ISO International Organization for Standardization. 14

IT Information Technology. 10, 12, 14, 15, 17, 25, 26

ITIL Information Technology Infrastructure Library. 15

JS JavaScript. 20

JSON JavaScript Object Notation. 6, 12, 17

MAC Media Access Control. 29

MCDA Multi-Criteria Decision Analysis. 13

MDR Managed Detection and Response. 26, 29

MFA Multi-Factor Authentication. 21

MGMT Management. 28, 30

MIB Management Information Base. 29

MKB Midden- en Kleinbedrijf. 3, 15, 16, 18

ML Machine Learning. 10, 26

MS Microsoft. 15, 16

MSP Managed Service Provider. 6, 17

NDR Network Detection and Response. 26, 28

NIC Network Interface Controller. 29

NIST National Institute of Standards and Technology. 3, 14, 17

NoSQL Not Only SQL. 6, 20

NPM Node Package Manager. 34

OAuth Open Authorization. 22

OS Operating System. 32

OTP One Time Password. 20

Pentest Penetration Testing. 6, 15

Q-ICT Quality ICT. 0, 3, 10, 12–18, 22, 25, 28

QaaS Quality as a Service. 3, 10–17, 20–23, 25, 32, 33

QL Query Language. 25

RAM Random Access Memory. 21

RDMS Relational Database Management System. 6

REST Representational State Transfer. 6, 17, 23–25, 30

RMM Remote Monitoring and Management. 6, 17

SaaS Software as a Service. 17

SDK Software Development Kit. 29, 30

SEM Security Event Management. 26

SIEM Security Information and Event Management. 14, 26, 28

SIM Security Information Management. 26

SME Small and Medium-sized Enterprises. 14, 16

SOAP Simple Object Access Protocol. 16, 17, 23–25

SOAR Security Orchestration, Automation, and Response. 26

SOC Security Operations Center. 26, 28, 29

SWOT Strengths, Weaknesses, Opportunities, and Threats. 13

TAP Test Access Point. 6, 26

TS TypeScript. 20

URI Uniform Resource Identifier. 24

URL Uniform Resource Locator. 24

UUID Universally Unique Identifier. 6

UX User Experience. 17, 32

vCPU Virtual Central Processing Unit. 21

VLAN Virtual Local Area Network. 28

XML Extensible Markup Language. 6, 17, 23

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 measures, and improve their overall service delivery.

SentinelOne emerges as one of the leading organization in the cybersecurity real, offering cutting-edge endpoint protection and threat intelligence solutions. It leverages advance AI and ML algorithms, providing comprehensive protection against malware, ransomware, and other cyber-threats. It is one of the must-have protection tools for business organizations looking to bolster their cybersecurity posture and safeguard their digital assets.

As the main topic of this graduation work placement project, the author has been tasked to integrate SentinelOne endpoint protection capabilities into the client company internal application, the QaaS app. The main objective of this project is to promote transparency more into Q-ICT clients by providing them with real-time data and visibility into their organizations, enabling them to make informed decisions and take proactive measures to protect their own digital assets and mitigate security risks.

1.2 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.

1.3 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.

1.4 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 SentinelOne API in Flutter compare to other Security Threat Platforms to ensure clear and insightful representation of threats?

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 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 capabilities.

- Sub-question #3: research into existing visualization techniques for JSON 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.

- 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, secu-

rity impact risk assessment, and feasibility checklist assessment with the Company Supervisor will also be overseen.

2.2.2 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.

2.2.3 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.

2.2.4 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 of SentinelOne integration for the GET request method only.

The author is also limited in showing the SentinelOne dashboard data, as it contains clients' sensitive information, and Q-ICT has over 400 clients. Therefore, if any part of the SentinelOne dashboard is shown, it will be with blurred sensitive information.

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

Before diving straight into the QaaS app, a general understanding about the company, Q-ICT is needed first to understand the context of the QaaS app and its place within the company that is using it.

2.3.1 The Company

Q-ICT, is a small cybersecurity consultancy based in Emmen, northeast of the Netherlands. The company follows a flat organizational structure, which means that there are few or no levels of middle management between the staff and everything communication directly goes with the director. 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. As of now, Q-ICT has over 400 active customers. Some of the notable clients are: Kigpolis Verzekeringen, CLS Europe, and Heli Holland.

Q-ICT 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.

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.

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 on his graduation workplacement 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 together 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.

Q-ICT Sister Companies

Q-ICT has 2 other sister companies who are also under the same ownership of Mark Kolk, which are MKBoT and QaaS.nu respectively.

MKBiT

It is a parent-company of Q-ICT who provides IT solutions and consultation to its clients. It was founded to support Q-ICT business operations. It shares the same office with Q-ICT. Its services include cloud solution, Microsoft 365 products, patch-management, online-backup, AV, anti-spam, and monitoring software applications.

Luuk Admiraal is directing this company. Because the company is an IT service provider, it has a vast network of suppliers and partners to provide them with the products and brands to support their business. Here is the list of the suppliers: DrayTek, HP, Microsoft, and Ubiquiti Network.

QaaS.nu

This company is responsible for the software development of Q-ICT. It is still a small company which was set up not a while ago, so there is not a lot of info feasible for the author to write about it. Their upcoming projects are still proof-of-concept. The company is directed by Pierre Kleine Schaars. This terminology is not to be confused with the QaaS app, which is the internal app of all the three companies.

Products and Subscriptions

Besides cybersecurity, together with MKBiT and QaaS.nu, Q-ICT offers a wide range of products and services to its clients. Those products are (*MKBiT, n.d.*):

- Customized software development: this field is one of the main responsibilities of Q-ICT itself, it provides customers with tailor-made software solutions that are designed to meet their specific needs and requirements. The company works closely with clients to understand their unique challenges and develop software applications that effectively address those concerns.
- Online-backup: the company offers a service where the clients can store copies of their files, documents,

and data on remote servers via the internet. These remote servers are hosted in secure data centres. Furthermore, MKBiT also provides DB migration in case any event of disasters occurred.

- Active monitoring: the company will offer its customers the chance to oversee, track, and manage their computer systems, networks, or applications in real-time. It serves various purposes, including ensuring system stability, optimizing performance, enhancing security, and providing valuable insights into the usage patterns and behaviours of users or devices. In the future, it wants to bring more automation to its system, providing customers with automatic messages when a disk space becomes full, or when there is an error message in clients' computers.
- Anti-spam software: a specific type of software application that is designed by MKBiT to detect, prevent, and block unsolicited and unwanted e-mail messages, commonly known as spam, from reaching clients' e-mail inboxes. They are typically sent in bulk to many recipients without their consent, often containing advertisements, phishing attempts, malware, or other malicious content. It has features such as whitelist, blacklist, and filter e-mails per e-mail account or e-mail address.
- Microsoft 365 products: the company is also providing access to Microsoft's suite of cloud-based productivity tools and services, including installation services, to its clients. These include Microsoft Word, Excel, PowerPoint, Outlook, and more, which are all accessible online through a web browser or can be installed on local devices such as computers and smartphones.
- AV software: it resells and gives clients advice and comparisons on good antivirus software from manufacturers like McAfee, Bitdefender, and Kaspersky. This software is designed to detect, prevent, and remove malware from computer systems.
- Cloud services: the company also provides clients with a tailor-made cloud solution based on their specific wishes and problems, whether it is using a public, private, or hybrid cloud. It delivers a range of computing resources, applications, and services over the internet through cloud computing technologies. These services enable the clients to access and use computing resources without the need to own or maintain physical hardware and software infrastructure, enabling their employees to access their files anytime, anywhere, without others having to access them.

In addition, for the software development, Q-ICT also uses other MS technologies such as Power Platform (i.e., Power Automate, Power BI, Power Apps, Power Virtual Agents, and Power Pages), Dynamics 365, and Azure to help with their software development, therefore the clients who are asking for the product to be developed with the help of those MS technologies will also have those subscriptions of the products, therefore paying extra charge.

The company also offers subscriptions, such as:

- QaaS Safe:
- QaaS Help:
- QaaS Backup:

Unofficial Partnerships

Q-ICT has several unofficial partnerships with other organizations, they are normally located in the same building that Q-ICT rents its office from. These organizations help Q-ICT in their own speciality, and Q-ICT helps them in return. These organizations are:

- MemoICT: is a Shopware company that helps with e-commerce (*MemoICT, n.d.*).
- Ondernemend Emmen: helps with international entrepreneurship, knowledge sharing, and networking (*OndernemmendEmmen, n.d.*).
- Peat Digital: helps with online marketing to promote Q-ICT products more into wider audience (*PeatDigital, n.d.*).
- Webba: helps with web development, especially designing Q-ICT, MKBiT, and QaaS.nu website (*Webba, n.d.*).
- InDiv Solutions: also helps Q-ICT with the front-end side of their website development (*inDiv Solutions, n.d.*).

APIs and Technologies

The QaaS app also utilizes several APIs and technologies to help with its operations. It needs to manage and make connection different sort of APIs to help with the operations of the an ERP application. Those APIs are the following:

- Resello: is used for Q-ICT MS subscriptions owned by Pax8 (*LinkedIn, n.d.*). 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. Furthermore, it normally uses SOAP API for its communication.
- 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. It normally uses REST API for its communication.
- 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.
- PerfectView: is used for CRM software (*PerfectView, n.d.*). It is designed to improve business relationships with customers, assist in customer retention, and drive sales growth. In the QaaS app, it is used to manage the relationships and interactions with the app's users, which could include tracking user interactions, managing customer support requests, and analyzing user data to improve the app's functionality and UX.

A deeper explanation of what these kinds of API are will be discussed in the later part of this research sub-question.

Besides all the 5 internal APIs that Q-ICT uses, the company also uses several technologies to help them with their operations. Those tools are:

- Computicate (now newly named Acronis): is used as their ticketing system, providing ticketing solution services to customers for a wide range of events and activities (*Acronis, n.d.*).
- TOMTelecom: is used for their company's phone system. It is responsible for structured process of call routing on incoming calls from customers to the appropriate department or individuals, ensuring effective communication and issue resolution (*TOMTelecom, n.d.*).

2.3.2 The QaaS App Infrastructure

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 to For Q-ICT employees themselves, 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.

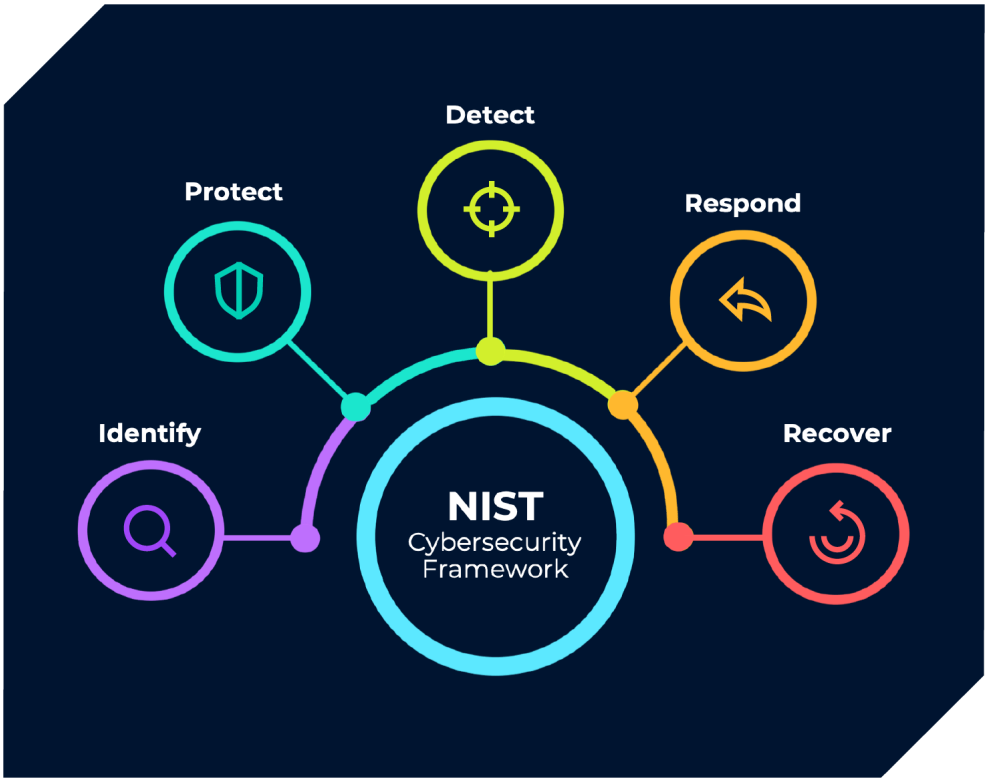


Figure 2.1: NIST working methodology that is followed by Q-ICT

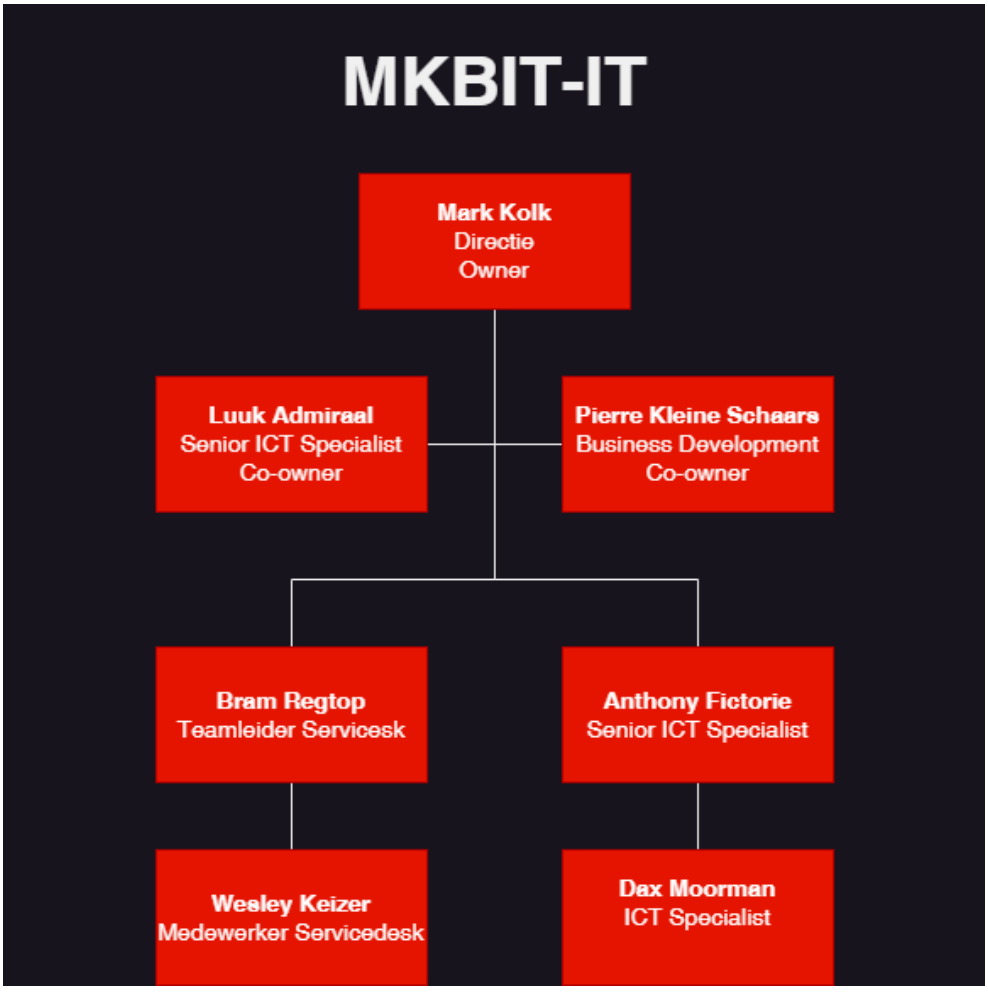


Figure 2.2: Level of structure of MKBiT

Figure 2.3: Flat (hierarchical) structure of Q-ICT

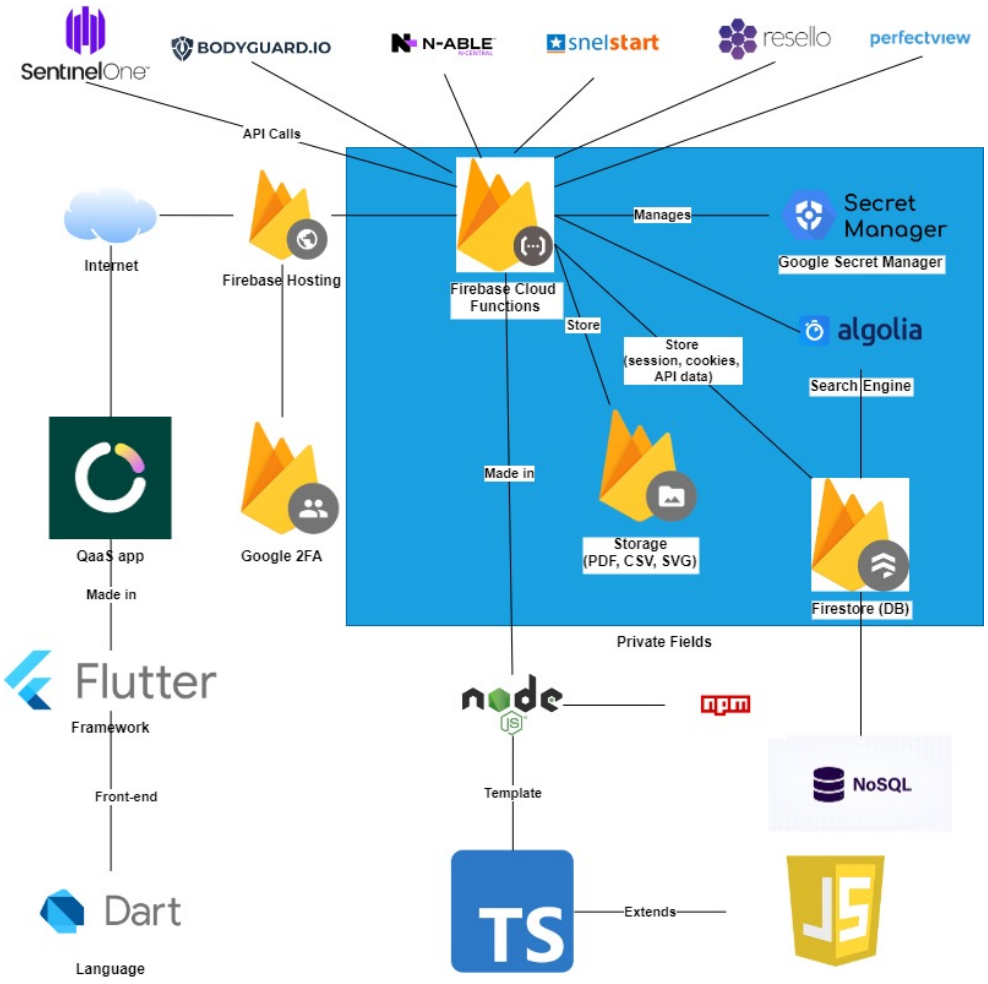


Figure 2.4: The infrastructure of the QaaS app

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.-i). It 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 (*Firebase, n.d.-c*) are many, but for this thesis, it will only discuss the ones that are used by the QaaS app. They are listed in the following:

- 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.
- Database:
  - 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.
- 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 is 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

  Cloud functions are the main back-end infrastructure of the QaaS app. It is used to connect and make HTTP calls to all the internal APIs. There are different types of functions in Firebase Cloud Functions, and they will be discussed later.

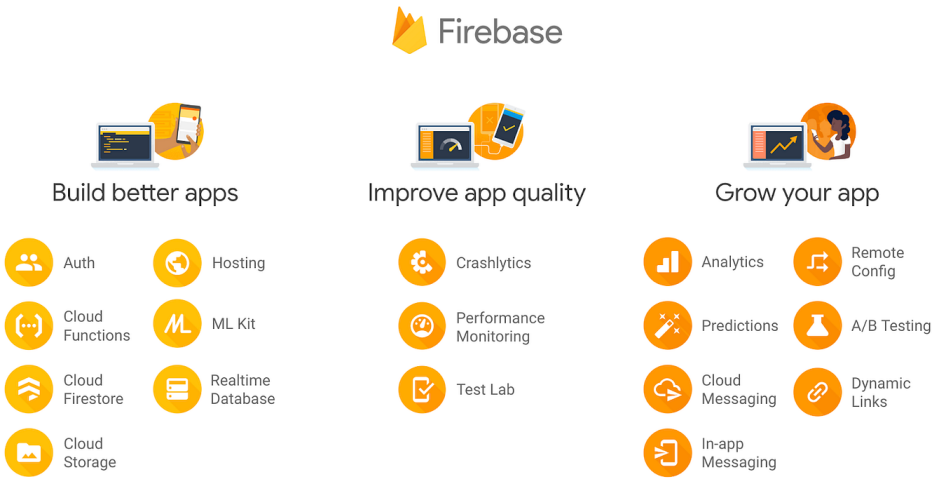


Figure 2.5: All of the products offered by Firebase (*Kubernetes, 2018*)

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

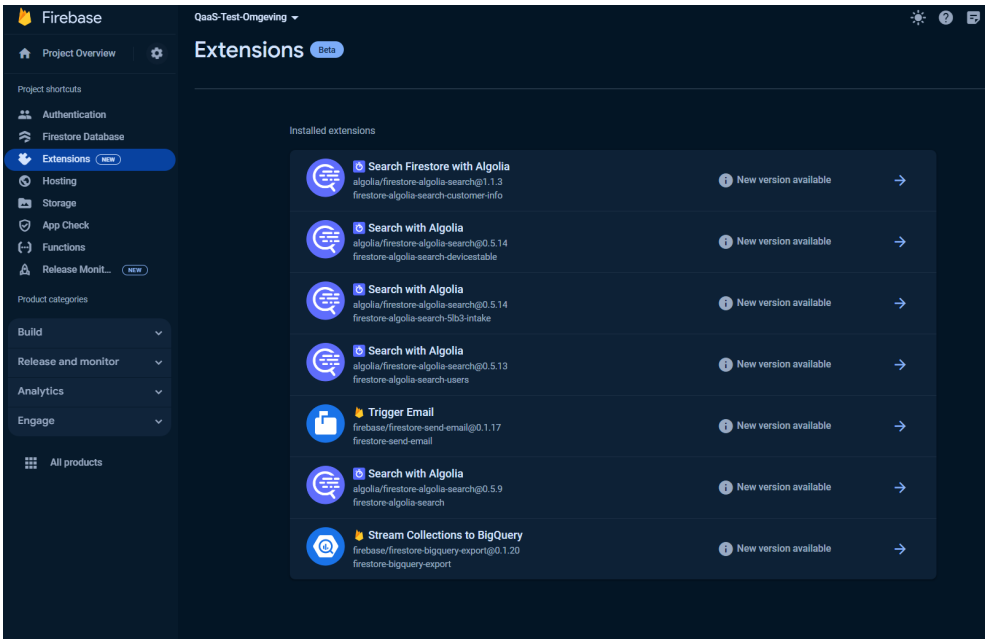


Figure 2.6: All the extensions that are used in the QaaS app, mostly about Algolia

Listing 2.1: Example of onCall function with authentication check

```
const region = "europe-west1";

const getData = functions.https.onCall({ region: region }, async (request: CallableRequest<any>) =>
    {
     try {
          // Checking that the user is authenticated.
          if (!context.auth) {
               // Throwing an HttpsError so that the client gets the error details.
               throw new functions.https.HttpsError('failed-precondition', 'The function must be
                    called while authenticated.');
          }
     }
     catch (ex: unknown) {
          if (error instanceof Error) {
               // Error object, log message and stack if available
               console.error(`[${context}] An error occurred: ${error.message} \n Stack:
                    ${error.stack}`);
          } else {
               // Non-Error object, log with a generic message.
               console.error(`[${context}] An unknown error occurred:`, error);
          }
          throw new functions.https.HttpsError("unknown", "Failed to retrieve agents", ex);
     }
```

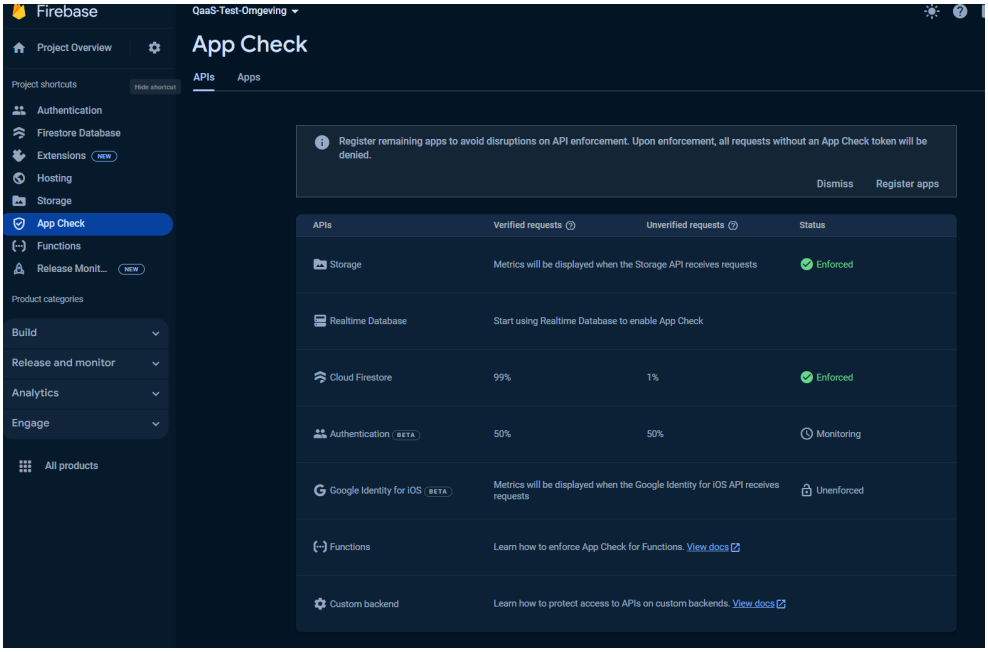


Figure 2.7: The App Check feature in the QaaS app

Figure 2.8: The function in the QaaS app that is scheduled to run every 7 days to keep the API data up-to-date (*Cronitor, n.d.*)

```
21      });
22
23      export = getData;
```

- 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 Storage: offers 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. It is used by the QaaS app to store and serve user-generated content, such as profile pictures, documents, and other files.
- Extensions: it consists pre-built, open-source software packages that extend the functionality of a Firebase project (*Firebase, n.d.-b*). They are designed to automate common development tasks, such as sending notifications, integrating with third-party services, and performing back-end operations, without requiring users to write custom code. The QaaS app uses the Extension mainly for Algolia.
- App Check: it is a security feature that, on top of Firebase 2FA Authentication, that helps protect the project from abuse, such as billing fraud or phishing, by ensuring that only the app that is registered can have access to the Firebase project's resources (*Firebase, n.d.-a*). In the case of the QaaS app, it uses it reCAPTCHA to ensure extra protection in the MFA.

Different Types of Cloud Functions in Firebase

Firebase has a lot of different types of Cloud Functions that developers can use. Just like the previous Firebase product explanation, this thesis will only focus on the following types of Cloud Functions that are used in the QaaS app:

HTTP Triggers: these are functions that are triggered by HTTP requests. They are used as API endpoints of the QaaS app, allowing server-side logic execution in response to HTTP requests from client-side applications or external services. The requests are GET, POST, PUT, DELETE, and PATCH, and they are used to creating, reading, updating, and deleting data in either the Firestore DB or the correlated API environment itself.

- onRequest:
- onCall: is a little different from onRequest. Instead of using Request and Response, it uses data

and context. In version 2.0, it only accepts request as `CallableRequest<any>` that can get any headers and body of the request sent by user. It is used to create Callable Functions, and they are designed to be called directly from client applications, such as mobile or web apps. They automatically handle authentication and data serialization, making it easier to secure call backend code from client applications, and this is what the QaaS app primarily uses for calling its internal APIs as it ensures that the client is authenticated and authorized to make the call. Callable functionsa are triggered by an HTTP request but are specifically designed to be called from Firebase client SDKs.

Pub/Sub Triggers

Cloud Firestore

Schedule functions: this is a Firebase's own term for Cron Job (*Firebase, n.d.-d*).

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.

Google 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 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.

Google Secret Manager comes from GCP, and GCP and Firebase are a separate cloud solutions. But, because both are part of Google, Firebase Cloud Functions can typically access GCP Secret Manager by editing that specific function that the developer wanted to grant access to.

Different Types of API By Audience

To understand better about the 5 internal APIs that are used by the QaaS app, including SentinelOne, it is important to understand the different types of APIs by its audience and protocol. There are 3 main types of APIs by audience, they are:

Public API: also called external or Open API, and as the name suggests it is available to everyone. They are open to 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 like 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. 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 2.2: 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.

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 2.3: 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 2.4: REST's Example Request

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

Listing 2.5: 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.

Modules and Templates of the QaaS App

The QaaS has several templates and modules that are used to build the app. The templates can be interpreted as level of access to the app, showing what permission a user has to the app. There are 3 different templates based on 3 different users:

- **Clients**: this template is used by the general users of the app. They have limited access to the app's features and functionalities, such as viewing and updating their profile and accessing the app's resources. They can only see the data relevant to their own account and cannot access or modify data belonging to other client from different company. The Client template is designed for users who have the lowest level of access and control over the app.
- **Helpdesk**: this template is used within the Helpdesk department of Q-ICT. They have more access to the viewing of app functionality than the Clients.
- **IT Admin**: the IT admin have almost the same level of access as the Helpdesk. The only difference is that they have the ability to create, edit, and delete users, manage user permissions, and configure the app settings. They can also grant and revoke access to a user and to the app's features and functionalities, which are called Modules. The admin template is designed for users who have the highest level of access and control over the app, which is to the developers.

Modules are

2.4 Research Sub-Question #2

2.4.1 SentinelOne

To answer this research sub-question, a general understanding of what SentinelOne is needed 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.

Examples of endpoints are:

- Computer (workstations, desktops)
- Laptop
- Server
- Mobile devices

EPP

EPP is an upgrade from legacy AV/anti-malware. EPP consists of solutions that work together to detect and block security threats at the endpoint device level.

Important note that EPP is not to be confused with EDR. EPP is a separate service from EDR, in which in EDR platforms they often include EPP but not vice versa.

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), thus operate only on endpoint level.

The number one thing that sets apart EDR from legacy (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 compared to only concerning with malicious software like what traditional AV does.

MDR

MDR is what manage the EDR technology.

NDR NDR products are designed to provide a complete visibility into the network, real-time detection of threats, and guided investigation to accelerate and automate responses (*SentinelOne, n.d.*). NDR takes a feed of raw network traffic from a Network TAP, port mirror, or virtual traffic mirroring in AWS and Azure. By analyzing this traffic in real-time, NDR finally discovers and classify every device communicating on the network. It identifies device roles, such as DNS, web server, medical device, etc., and maps peer groups among those devices.

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 (Gartner, 2017). SIEM tools evolved from the log management discipline and combine SIM and SEM technologies. A SIEM tool uses AI to automate several 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, firewall, IPS, IDS, and EDR data
- Output: high-fidelity alerts prioritized by severity
- Infused with: AI, ML, and analytics

SOAR

SOAR solutions focus on automating incident response processes and triage capabilities. The key word here is "orchestration" and "automation". In an ideal world, everything. The main goal is to oversee security without human help as much as possible, boosting productivity and shortening 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.

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 even deal with hidden and advanced malware.

MXDR

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

SOC

SOC is the organizational context itself. It is a centralized facility or team within an organization that houses a security team responsible for monitoring and analyzing another organization's (client) security position on an ongoing basis. They can be seen as the safety team for client organizations. Please note that SentinelOne company itself is not a SOC, as it is just a cybersecurity company that offers endpoint security solutions.

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. In terms of SentinelOne, it has all the features that are mentioned in the diagram, except for SOC, as was mentioned before.

Console

Global

The Global tab refers to the environment of the highest level of advisors. It consists of organizations that have access to global level that propagate down to the tenant level, which means they can put policies, scripts, and other configurations that will be applied to all console and all of their customers.

Tenant

Mentees

Site

Site is just a name

Group

Group refers to logical grouping of devices within SentinelOne MGMT Console. Groups can be created and deleted by the admin user, and

Agents

An Agent is a software program, part of SentinelOne product, that is 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,

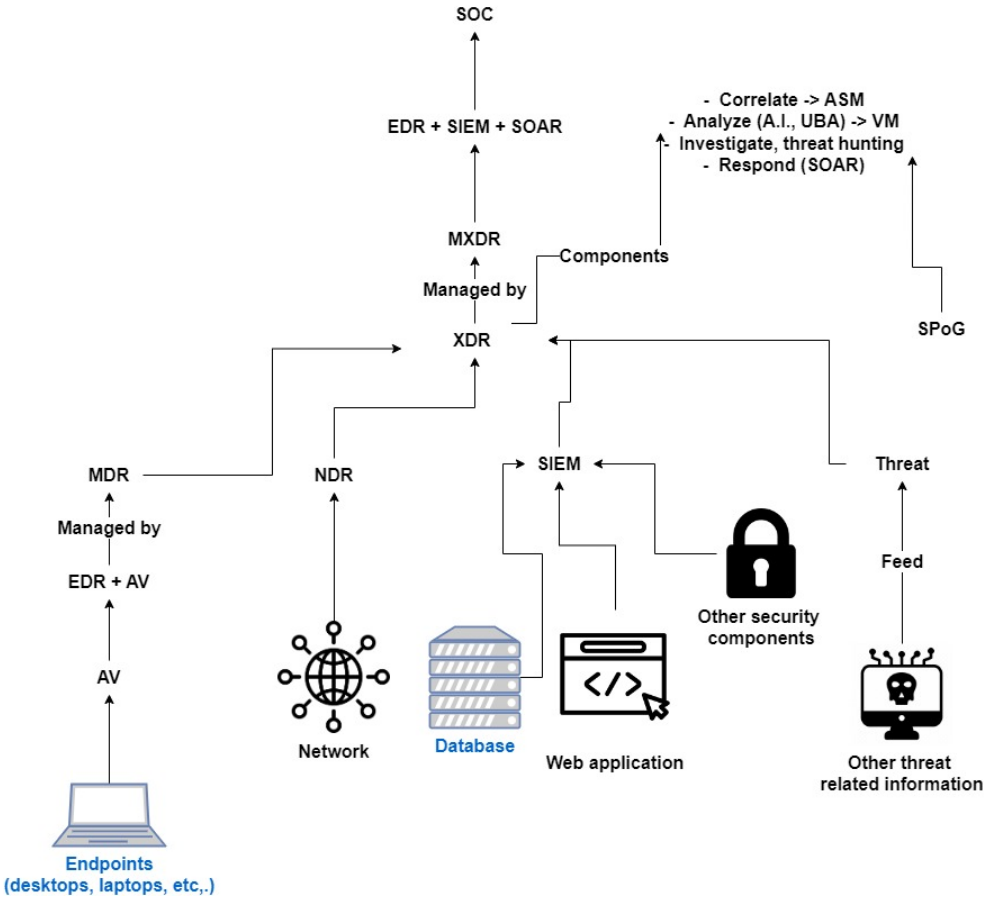


Figure 2.9: How all terms related to various technologies in cybersecurity connected to each other

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).

Ranger

Ranger is an add-on 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 that 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.

- Not reviewed
- Not trusted
- Under analysis
- Allowed

Ranger is designed to detect and take out malicious actors that are in the local subnet, as they can a lot of information about the devices (*see ARP Poisoning Wikipedia, n.d.-c and man-in-the-middle-attack Wikipedia, n.d.-j*). In the real-business scenario, a lot of the times, a company has a very secure perimeter firewall (*the big outer castle wall in castle-and-moat network security model Taylor, 2021*), but the inside network are wide open (unless they are doing logical separations of their local network, such as using VLAN) for attacks inside the network.

Unfortunately for this project scope, Ranger API calls are off limit, as the company is still..., therefore displaying all the Ranger ability to scan and the API call of the author's account.

Sentinels

Sentinels refer to a term that describes SentinelOne ability to deploy and manage security agents on endpoints within an organization, not part of SentinelOne product, like Ranger. This is part of the SentinelOne EDR capabilities, where the user admin can deploy the agents on the endpoints, and manage them from the SentinelOne console. The admin can also create policies, scripts, and other configurations that will be applied to all the agents in the network.

Visibility

Unfortunately, Q-ICT does not have Visibility turned on its tenant, thus this feature is also off limit for this project scope. But in general, Visibility allows users to do deep querying to be able to identify different things, such as attributes of a machine. It is useful when user is looking for threats or any additional information in Incident Response or Threat Hunting, which in most cases is proactive, Visibility can give the user a lot of power to use queries, and interrogate all the information or telemetry that SentinelOne has pulled off from the connected machines.

Incidents

Incident is just a name of a page in SentinelOne dashboard that provides a list of cyber-incidents overview that have happened on all endpoints detected by Agents in the network connected to SentinelOne by Ranger. The page typically offers an overview of all detected security incidents, categorized based on severity levels of types of threats.

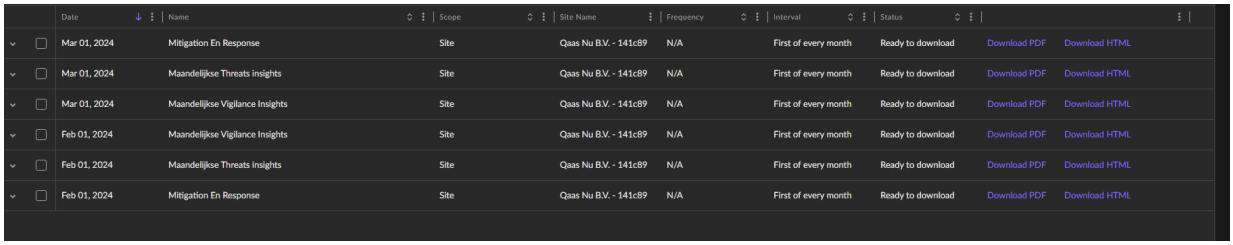
Once a threat is detected, the user can take the following actions in the dashboard, if they have enough privileges to do so:

- 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 taking 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 been executed.

Reports

The reports in SentinelOne provide users with insights into the security posture and threat landscape across their organization's endpoints. The reports offer customizable reporting capabilities, allowing users to generate reports tailored to their specific requirements. Users can then choose from a variety of predefined report templates or create custom reports based on their unique needs.

Furthermore, the users can also choose for the report to be made automatically, instead of manually filling them themselves. They can schedule automated report generation at regular intervals, such as daily, weekly, or monthly.



Date	Name	Scope	Site Name	Frequency	Interval	Status		
Mar 01, 2024	Mitigation En Response	Site	Qaas Nu B.V. - 141c89	N/A	First of every month	Ready to download	Download PDF	Download HTML
Mar 01, 2024	Maandelijkse Threats insights	Site	Qaas Nu B.V. - 141c89	N/A	First of every month	Ready to download	Download PDF	Download HTML
Mar 01, 2024	Maandelijkse Vigilance Insights	Site	Qaas Nu B.V. - 141c89	N/A	First of every month	Ready to download	Download PDF	Download HTML
Feb 01, 2024	Maandelijkse Vigilance Insights	Site	Qaas Nu B.V. - 141c89	N/A	First of every month	Ready to download	Download PDF	Download HTML
Feb 01, 2024	Maandelijkse Threats insights	Site	Qaas Nu B.V. - 141c89	N/A	First of every month	Ready to download	Download PDF	Download HTML
Feb 01, 2024	Mitigation En Response	Site	Qaas Nu B.V. - 141c89	N/A	First of every month	Ready to download	Download PDF	Download HTML

Figure 2.10: Examples of automatic reports that can be downloaded in SentinelOne

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.

The company wishes

How does SentinelOne get all this information from a device without having them even connected to the Internet?

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. As everything that is talking on Layer 2 is giving out their MAC address for exchange,

A lot of the times, most switches and routers do not change their default credentials

As was said before, every single item that is connected to a network is constantly broadcasting information out to the rest of network, in order to get and maintain an IP address to keep accessing the Internet, even when it is not actively using it (*see DHCP Protocol Gillis, 2023*). In case of an endpoint that has SentinelOne installed on it that has Ranger, that Ranger is going to listen to that NIC on that device, then capture and interpret all the data that is flowing across the network, called MIBs, thus displaying it on the Console.

2.4.2 SentinelOne API & SDK

SentinelOne provides both an API and an SDK to allow users to integrate SentinelOne with other security tools and systems. The SDK is called Nexus Embedded AI (*Anfalovas, 2022*), which enables organizations to scan files and detect malicious content among them.

Listing 2.6: SentinelOne SDK implementation

```
from SentinelDFI.scanner import *
s = Scanner(True)
verdict = s.scanFile("/home/test_me/malicious.docx")
```

```
File hash: 421ac4189Seed605824fc4cae3e60219febfef
Verdict: malware
Score: 0.297529
Indicators: `Detected VBA Structure,Encrypted file,Encrypted Word Document,Has DDE`
```

Besides SDK, SentinelOne also provides a RESTful API with its comprehensive documentation that allows users to interact with the SentinelOne platform programmatically. The API provides a wide range of functionalities, including the ability to retrieve information about devices, incidents, and threats, as well as the ability to perform actions such as quarantining devices, remediating threats, and generating reports. The API is designed to work with the Agents, Sentinels, Ranger, and other components of the SentinelOne platform.

There are many techniques that can be used to create a link (often called an interface). The technology for linking to SentinelOne depends on the **purpose** and **capabilities** of the software to be linked:

- **REST, SOAP API/ Webservice**: modern software has its own inputs and outputs to exchange information. This is a sustainble and solid solution for the processing of data
- **CSV/XLSX and XML via (S)FTP**:
- **Webhooks**: like web services, but event based. A signal is automatically sent for each mutation, so that action to process the signal within the software can be taken.

API Token

To be able to access SentinelOne APIs, the user needs to have an API token to prove their identity and that their organization has SentinelOne subscription, therefore has right to access data. API tokens can be created in the SentinelOne MGMT Console.

The API token will be shown only once; therefore the user needs to store it in a secure place. The token generated by the user is time-limited. To renew the token, the user must generate a new one with the same above-steps.

API Token Storage

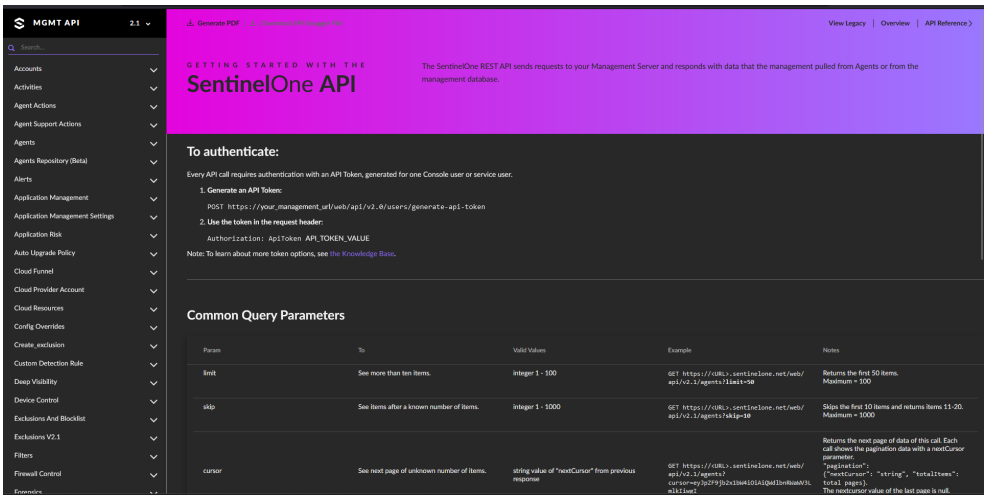


Figure 2.11: SentinelOne API Documentation

2.5 Research Sub-Question #3

Data visualization is the process of representing complex data (in the form of text and numbers) into a graphical representation, such as: interactive charts, dashboards, pie charts, and so on. In the context of this project, the displays should be able to tell interesting stories and share findings with diverse audience (the client, helpdesk, and cybersecurity analysts).

2.5.1 Data Visualization Widgets in Flutter

In Flutter, there are 2 famous library that supports a wide range of chart types, fl_chart and syncfusion_flutter_charts. Each chart type is suitable for a specific kind of data and provides a different way to visualize the data. Types of charts in both libraries include 30+ plotting series:

- Line chart: is used to display data points connected by straight line segments. They are commonly used to show trends over time.
- Bar chart: it uses rectangular bars to represent data. The length of each bar corresponds to the value it represents. Bar charts are useful for comparing quantities of different categories.
- Pie chart: represents data in the form of slices of a pie. Each slice corresponds to a category of the data, and the size of the slice is proportional to the quantity it represents.
- Scatter chart: uses dots to represent data points on a two-dimensional plane. They are useful for showing the relationship between two variables.
- Radar chart: A.K.A. spider chart or star chart, is a way of comparing multiple quantitative variables. This makes them useful for seeing which variables have similar values or if there are any outliers among each variable.

Each chart type is easily configured with built-in support for creating stunning visual effects, and any number of series can be added to the chart. Features such as markers, data labels, data label builder, animation, gradient fill, dashes, sorting, and annotations are easy to incorporate and customize.

Several main components of each chart type are:

- Chart data: the most important part is the data wanted to be displayed. This could be a simple list of numbers, or more complex data structure, depending on the type of chart.
- Chart type: the second most important part is to specify the type of chart.

Figure 2.12: Chart types in Flutter fl_chart

- Axes: the x and y-axes of the chart. The axes provide a reference frame for the data points and can be customized to suit user's needs.
- Grid: the grid lines on the chart. These lines can help users better understand the data by providing a reference frame.
- Touch response: the way the chart responds to user's touch events. It can be customized by providing different types of interactivity, such as highlighting a data point when it is touched.

Axis Types

Axis features such as label intersecting, edge label placement, label rotation, axis opposition, inverse axis, and multiple axis allow users to customize axis elements to make an axis more readable. Four of the axis types that are supported are:

- Numeric
- Category
- Date-time
- Logarithmic

User Interaction

The package greatly enhance UX by adding the following functionalities:

- Zooming and panning
- Crosshairs
- Trackballs
- Drilling down
- Events
- Selection
- Tooltips

Legend

The package also supports legends, which display additional information about a chart series. The legends can be used to collapse the series and can be wrapped or scrolled if items exceed the available bounds.

2.5.2 Comparison to other EDR solutions

To determine the best visualization techniques for SentinelOne, a comparison to other EDR solutions is needed. In this section, the author has looked into other alternatives to SentinelOne, which are a single EPP/EDR solution, created as a complete replacement of legacy AV. Please keep in mind that in this subquestion, 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.

Heimdal®

On the homepage, information about each of the products/modules that are active under the current customer account is shown. The chart, which can be seen include a variety of Bar charts, Pie charts, and Line charts, include data regarding attacks, vulnerabilities, detections, infected/quarantined files, blocked/allowed processes, third-party application vulnerabilities or OS updates, and quarantined/rejected e-mails.

CrowdStrike

Trend Micro

Trend Micro Apex One has customizable contents and layout of their dashboard. Workload Security uses Session to save user's settings and remember the last view of the dashboard the next time the user log in. The colour here is a bit basic with only the typical red, green, blue, and yellow.

Based on the three examples above, some conclusion can be drawn about the techniques they use in their dashboard:

Visualization techniques

All three solutions use a combination and types of bar charts, pie charts, and line charts to display data. This due to the fact that the type of data they are trying to display is categorical and numerical data. Categorical data is data that can be divided into distinct groups or categories with no inherent order, and one category can only have one value.

Pie charts are used to visualize relative proportions or percentages of different categories within a dataset. Each category is represented by a slice of pie, with the size of each slice corresponding to the proportion of that category relative to the whole dataset.

Bar graphs are used to compare the quantities or frequencies of different categories. Each category is represented by a separate bar, with the height (or length, in horizontal bar graphs) of the bar indicating the value of that category.

In the case of SentinelOne integration to the QaaS app, both bar and pie charts can be used with the addition of line charts to display the timeline of a Threat Incident, and Scatter charts to show the relationship between two variables.

Customizable Widgets

All three solutions allow users to customize the layout and contents of their dashboards. This is important as different users may have different preferences and requirements for the data they want to see. Customizable widgets allow users to choose which data they want to

display, how they want to display it, and where they want to display it on the dashboard.

The SentinelOne dashboard of the QaaS app should have this functionality, therefore it should store user's preference **Coloring**

Chapter 3

Realization

Firebase Cloud HTTP GET

SentinelOne NPM package

3.1 Synchronization with N-Central API

Chapter 4

Conclusion and Recommendation

4.1 Conclusion

Cybersecurity is a complex field and threat actors are ever evolving their trade-craft in clever ways. Every single running business is not too small to be attacked, but they may be too small for them to make the news. Therefore, transparency to the clients is important, because lack of visibility

4.2 Recommendation

Bibliography

Acronis. (n.d.). Computicate. *solutions.acronis.com*. https://solutions.acronis.com/en-us/integrations/computicate/

Anfalovas, I. (2022). What is address resolution protocol? a beginner's guide to ar. *Ipxo*. https://www.ipxo.com/blog/address-resolution-protocol/

Cronitor. (n.d.). Crontab guru. *contab.guru*. https://crontab.guru/#0_0_*/7_*_*

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.-a). Firebase app check. *Firebase.google.com*. https://firebase.google.com/docs/app-check

Firebase. (n.d.-b). Firebase extensions. *Firebase.google.com*. https://firebase.google.com/docs/extensions

Firebase. (n.d.-c). Firebase products - google. *Firebase.google.com*. https://firebase.google.com/products-build

Firebase. (n.d.-d). Schedule functions. *Firebase.google.com*. https://firebase.google.com/docs/functions/schedule-functions?gen=2nd

Gartner. (2017). Security information and event management. *Gartner Research*. https://www.gartner.com/en/information-technology/glossary/security-information-event-management

Gillis, A. S. (2023). Dhcp (dynamic host configuration protocol). *TechTarget*. https://www.techtarget.com/searchnetworking/definition/DHCP

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/

IBM. (n.d.). What is a rest api? *CyberHoot*. https://www.ibm.com/topics/rest-apis#:~:text=A%20REST%20API%20(also%20called,transfer%20(REST)%20architectural%20style).

inDiv Solutions. (n.d.). Indiv solutions focus op online webshop laten maken. *indiv.nl*. https://webba.nlhttps://indiv.nl/

Kubernetes. (2018). Cronjob. *kunbernetes.io*. https://kubernetes.io/docs/concepts/workloads/controllers/cron-jobs/#:~:text=A%20CronJob%20creates%20Jobs%20on,schedule%2C%20written%20in%20Cron%20format.

LinkedIn. (n.d.). Resello: Powered by pax8. *LinkedIn.com*. https://www.linkedin.com/company/resello-bv/

MemoICT. (n.d.). Home | memo ict | de shopware specialist. *memo-ict.nl*. https://memo-ict.nl/

MKBiT. (n.d.). Service centraal. *MKBiT.nl*. https://mkbit.nl/producten/

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

OndernemmendEmmen. (n.d.). Ondernemend emmen: Home. *ondernemendemmen.nl*. https://www.ondernemendemmen.nl/

PeatDigital. (n.d.). Home | peat digital| specialisten in online marketing. *peatdigital.nl*. https://peatdigital.nl/

PerfectView. (n.d.). Pefectview crm online | krachtige nederlandse crm. *PerfectViewCRM.nl*. https://www.perfectviewcrm.nl/

SentinelOne. (n.d.). What is network detection and response (ndr)? *SentinelOne®*. https://www.sentinelone.com/cybersecurity-101/what-is-network-detection-and-response-ndr/

Taylor, C. (2021). Castle-and-moat network security model. *CyberHoot*. https://cyberhoot.com/cybrary/castle-and-moat-network-model/

Taylor, C. (2024). Castle-and-moat network security model. *CyberHoot*. https://cyberhoot.com/cybrary/castle-and-moat-network-model/

TOMTelecom. (n.d.). Wie zijn wij. *tomtelecom.nl*. https://www.tomtelecom.nl/wiezijnwij/

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/

Webba. (n.d.). Webba | experts in design, techniek en online marketing. *wenbba.nl*. https://webba.nl/

Wikipedia. (n.d.-a). Algolia. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Algolia
Wikipedia. (n.d.-b). Api. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/API
Wikipedia. (n.d.-c). Arp spoofing. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/ARP_spoofing
Wikipedia. (n.d.-d). Captcha. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/CAPTCHA
Wikipedia. (n.d.-e). Captcha. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/ReCAPTCHA
Wikipedia. (n.d.-f). Customer relationship management. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Customer_relationship_management
Wikipedia. (n.d.-g). Cyber threat hunting. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Cyber_threat_hunting
Wikipedia. (n.d.-h). Enterprise resource. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Enterprise_resource_planning
Wikipedia. (n.d.-i). Firebase. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Firebase
Wikipedia. (n.d.-j). Man-in-the-middle attack. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Man-in-the-middle_attack
Wikipedia. (n.d.-k). Penetration test. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Penetration_test
Wikipedia. (n.d.-l). Remote monitoring and management. *Wikipedia, free encyclopedia*. https://en.wikipedia.org/wiki/Remote_monitoring_and_management