- Can you provide me with details of what kind of QaaS subscriptions we have? (is QaaS Safe, QaaS Help, and QaaS backup)

Subscription within the QaaS app is divided into smaller proportions (all monthly subscriptions):

- QaaS Safe: security package, patch management, monitoring for workstations or laptop, traditional AV (BitDefender) => will be removed soon as SentinelOne EDR itself is already an upgrade from traditional AV. This subscription is required for every user in a company. SentinelOne payment subscription is also included in this.
- QaaS Safe +: for advance security protection. Bodyguard.io is included. Still a proof of concept
- QaaS Help: for free call service to the helpdesk between working hours. For tracking if a user has this subscription or not financial DB like SnelStart and Computicket is used for billing users who do not have this subscription
- Back-up: for back-ups from the data of the customer from MS 365 Cloud provider. It is for restoring data if lost, stored off-site. It has a collaboration with N-Central

- Can you provide me with details of what kind of Microsoft 365 subscriptions we have? Do we only re-sell Microsoft 365 products to the clients? What makes them want to buy them from us and not directly from Microsoft itself?

We resell Microsoft products from Pax8, a Microsoft provider. In general, you can look at what Microsoft offers for their products' subscriptions, and they will be like us.
They want to buy from us because we also provide support, assistance with installation, we can also directly contact Pax8 for help if some issues occur. Meanwhile, if the customers buy the subscriptions from Microsoft themselves, when they need help, they need to wait in the customer service line for a long time.

- Can you provide me with details of what kind of internet connection subscriptions we have? How do they work?

We offer solutions to the customer in terms of their internet connectivity, we also might get into contact with Internet providers, like KPN and Ziggo.

- Can you provide me with details of what kind of password manager subscriptions we have? How do they work?

For that subscription we are utilizing Keeper, which is a password manager product that requires paid subscription. Under the hood, in which most of us cannot see, Mark and Robbert can compare all the passwords being stored there from a user's account. If there is password duplication, or the passwords themselves are weak in complexity or length, they will advise customers to change their passwords.

- When a customer pays us for our subscriptions, does mean that they also pay subscriptions from SentinelOne, N-Central, Bodyguard.io, SnelStart, Resello (Pax8), and PerfectView (also KPN and Ziggo?)?

Yes

- With all the tools that we have in our disposal, how do we come up to our customers and offer them security protection as a cybersecurity consultant company? Can we be seen as an intermediary between SentinelOne and the customers?

Quality ICT is a cyber-security company. It helps customers with security questions, network providers, to guide our customers with security posture, analysis of a customer like cybersecurity incident response, what is security posture in MS 365, what needs to do to be cyber compliant compliant in the future.

MKBiT is an MSP (Microsoft Service Provider) that provides devices MS 365 for customers, answers all their IT related questions. The Helpdesk is not necessarily equiped with

cybersecurity knowledge, despite being part of Q-ICT, for that they need to go to Mark and Robbert.

- Are there any subscriptions that I missed?

SecureMe2: which is a security solution for security appliances. Like Bodyguard.io, it also comes from a Dutch company. It has a machine that connects to a network desired network, it then scans the whole network if sees suspicious traffic then report to Andre or Robbert, if for example a laptop has connection in botnet, if a malicious USB driver has been plugged into a network (same as SentinelOne Ranger?).

Additional questions

- Because we are a Microsoft company, does that mean the protection that we offer only limited to the Microsoft products? So, for example, if an attack happens but on Unix or MacOS machine, does that fall out of our scope then? Can SentinelOne be installed and working on a device that is not in Microsoft Windows?

Our knowledge is focused mainly on Microsoft. Customers with Unix or Mac OS computers may come and subscribe to us, and we will do our best to answer their cybersecurity questions.
But yes, SentinelOne can in fact be installed in a Unix machine.

- In case of a threat happens that is already not detected and mitigated by SentinelOne and caused problems in a customer's devices, what do we do then? Do one of our helpdesk/ cybersecurity experts comes directly to the client to handle it? What happens when they also do not know what to do? How dependent are we on SentinelOne? Do we have back-up for every customer that we have? Because last time Manuel told me we had over 400 customers, so that would make the back-up data very big.

SentinelOne should pick it up when a malicious threat happens.

Protect: What we do is that we inform the customer, turn off some devices, plug out ethernet, we may come to them to assists physically.
Investigation: we write document about the cyber threat that have happened. How many devices infected, how many data is lost, what kind of lessons that we learn from them.
Remediate

- Also relating to the QaaS app, you said it should send a notification to the specific users in the form of e-mails when a threat happens, do you also want the admin to customize the recipient of these e-mails? Do you also want an alert from the QaaS app itself?

For the Helpdesk, it should be used as a single panel of glass. The QaaS App needs to display what kind of incident happens, so the helpdesk knows what to do with it.

- You also said that for the helpdesk, the QaaS app should also guide them on what to do in case of a cyberthreat happens on a client's machine, can you elaborate more on this? Does SentinelOne API itself provide some sort of guidance to this?

By displaying the overview of the incidents that have occurred, the Helpdesk can then know what steps to take themselves.
Also, we expect that the SentinelOne page to be scalable. Adding new modules to the QaaS app will not be that hard, possible to do so in the interface, and delete old modules without crashing the program.

- Can you provide me with an explanation of what SentinelOne Vigilance is? What sort of implementation do you wish to be done for the QaaS app to have this ability as well?

Vigilance is an additional module for SentinelOne. It is 24/7 SOC, that has employees from another country monitors SentinelOne data during the work off-hours from that

specific country. Because hackers are relentless, they are oftentimes making use of work hours to do their malicious activities.

This is still proof of concept. Mark and Robbert are still investigating about it. So, this is an optional, if not out of scope, part of my graduation project.