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

QaaS propotitions:

QaaS Safe: security package, AV (BitDefender), patch management, monitoring, for workstations or laptop, monthly service, how many users they have for every users,

QaaS Safe +: for bodyguard, still in proposition, advanced protection, more secure package

Help: monthly subscription, call service desk between working hours, costs nothing to call, if not they need to pay, Financial DB like SnelStart, integrated in Computicate

Back-up: for back-ups from the data of the customers, almost everyone works in cloud, MS 365 Cloud, restore data if lost, stored off-site, monthly subs, part of 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?

A lot of different subs, different packages included

Resell them from Pax8, provider,

What makes them buy from us: support, there is a problem with subs, if customer cant access mail then we can Pax8,

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

One internet connection from office,

Offers solutions to the customer, get a contact with provider, like KPN, Ziggo,

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

Keeper needs to pay, comparing the passwords with score, for advising,

Different product.

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

Yes (SentinelOne, Bodyguard.io)

Patch management, device is up-tp-date as possible,

All the network devices, switches, routers get updated

* 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: a security company, 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 compliant in the future

MKBiT: MSP, provides devices MS 365 for customers, with IT questions as possible,

* Are there any subscriptions that I missed?

SecureMe2: security solutions, appliance, a machine that connects to a network, it scans the whole network if sees suspicious traffic then report to andre or robbert, if for example a laptop has connection in botnet

Also, there is a question not related to the subscriptions, but to SentinelOne. I’ve asked Manuel directly, but he directed me to you instead to answer it better:

* 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 MS, main focus,

Our best effort,

* 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,

Inform the customer, turn off some devices, plug out ethernet, come to (first thing: protect)

Investigation: document, how many devices infected, how many data is lost, what kind of lessons

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 to use as a single pane of glass, what kind of incident happens so they know 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?

They need to know the min info, know what to do, simple overview which incidents have happened on which subfolders,

**Extra question**

* 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?

Additional module for SentinelOne 24/7 SOC, off-work hours someone from another country monitors SentinelOne data and make use to that.

What’s part: SentinelOne page needs to be scalable, to add modules to the interface, and delete without crashing the program,

RangerL extra module, company with EDR devices, if EDR have Ranger, scans the whole network for Rogue devices, have USB state plugged, the Ranger will detect. It costs for extra license.