* (Can you tell me more about SentinelOne?)
* What is the primary objective of the integration of SentinelOne to the QaaS app? What issues do the QaaS app currently have that you hope SentinelOne will address in the future?

AV

Traditional: defined set of vulnerabilities

EDR: monitors traffic, reactions (like botnet on network) learn by pattern, benefits to ISO 27000 certification

Customer: Offer transparency to customers (open app from phone) and see status, their own status

Helpdesk: see all customers

IT

* Are there any specific functionalities or data points within the SentinelOne API suite that you believe are essential for achieving that goal in the QaaS app?

Customers (site): amount of devices that is protected, amount of infected endpoints

Helpdesk: what they need to do in terms of incidents,

* Are there any KPIs (Key Performance Indicators) that should be tracked over time to assess the effectiveness of the progress? Any functionalities/features that you think the QaaS app should be prioritized for this project?

Endpoints are protected

* In the event of a cybersecurity incident or breach detected by SentinelOne, how do you expect the app should behave or handle this situation to mitigate the impact and restore security? What error messages do you imagine should be displayed?

Alert by mail, could have: warning sign

Customers: also warning, maybe: popup messages

* Are there any common cybersecurity vulnerabilities or threats that the QaaS app should aware and be vigilant about relating to SentinelOne APIs? Especially when it comes to monitoring clients’ devices and giving insights into their security status.
* There are different roles of user management in the QaaS app (service desk, developers, clients), who is the target intended users here? How would you expect them to see the data? Do their needs and access levels of information differ? If so, how?

Customers: Monthly overview

* How do you envision the data obtained from SentinelOne being visualized within the QaaS app? What are your thoughts about the data visualization we already have regarding all the other 4 APIs (Bodyguard, N-Central, Pax8, SnelStart) in the QaaS app?
* Are there any data visualization techniques you prefer over another for conveying insights to both Q-ICT helpdesk and its clients to help them understand the data better? (i.e., Pie Chart, Line Graph, Bar Graph, Bullet Graph, etc.,)
* How do you imagine the SentinelOne page of the QaaS app will look like from usability and user experience perspective? Should the app prioritize user-friendliness and avoid excessive technical complexity as possible for the clients but not for the helpdesk?
* Are there any specific security protocols or procedures that should be followed for ongoing maintenance and optimization after this project is finished?

Check for privacy issues, everything is tested

* Are there specific features, recommendations, or anything that you would like to add? Any cybersecurity considerations and best practices that should be kept in mind?

Pierre:

Customers:

Servicedesk:

IT:

By integrating SentinelOne we show that we are complying a lot of regulations, ISO 27000, NIS2

Analyst verdict: servicedesk (mark incident as false positive)

Give a lot of information, nice colors

Quantity of services