

- Can you explain to me what QaaS app is? What does it do, what are the key functionalities it offers? How critical is it in the overall operations and services of Q-ICT?
  - What would you say the organizational user role structure of the QaaS app is? (developer, helpdesk, client user) What privileges do each of this user role management have?
  - What are the functionalities from the Firebase that the QaaS app currently utilizes? What are the other existing libraries or tools that are already integrated into the app? (flutter, node.js, firebase)
  - Currently, what are the challenges or limitations in the QaaS app, if any?
  - Can you provide insight architecture and design considerations of the QaaS app, regarding Firebase, Flutter, and the third APIs?
  - Can you explain to me all the 6 Q-ICT's internal APIs and what functionalities do they have? Currently, how are these APIs monitored/managed in the QaaS app?
- 
- What issues and challenges do you think would be the most significant if the QaaS app lacks proper standardized API monitoring?
  - What specific challenges or issue points you experienced while implementing these APIs into the QaaS app and while maintaining it?
  - Are there any dependencies or third-party services that the standardized API monitoring solution needs to interact with besides Firebase?
  - What are the expectations, desired outcomes, key metrics, and success criteria from the proposed enhancements to the API monitoring solution of the QaaS app along with SentinelOne integration? (any key points that the developer should prioritize and/or beware)
  - What data or insights would be the most valuable to visualize from SentinelOne? How do you envision the integration of SentinelOne into the QaaS app?
  - In your opinion, how should the QaaS app handle expired API keys? In what way?
  - Is there any budget set for this project?
  - Is there any code conventional style guidelines or specific security concerns relating data privacy or compliance that the intern should adhere to? What is the security best practices and testing procedures currently followed in the development of the QaaS app?
  - Are there any key challenges you are anticipating in the development of API monitoring and SentinelOne integration while maintaining highest security standards? Any specific areas of concern or potential risk?

- Why hasn't the SentinelOne be integrated in the QaaS app so far? Is it because the data shown is more complex? Different?
  - What strategies were employed for secure storage and management of API keys within the QaaS app and how effective were they?
  - Currently, how do the QaaS app handle any unsuccessful API calls or errors? Any error handling or logging?
- 
- How is the data retrieved from the current APIs visualized within the QaaS app? Are there any specific visualization needs or preferences for different departments/user groups? How user-friendly is the data representation and retrieval in the QaaS app according to you?
  - What visualization techniques have you used for the current APIs that you think have been the most successful or unsuccessful in the past?
- 
- What are the expectations for the integration of third-party APIs in the future? Are there any specific APIs you are planning to integrate, and what are the key requirements for their integration?
  - What are the overall goals of the QaaS app in terms of API management and cybersecurity monitoring? How do these goals align with the objectives of Q-ICT?
  - Are there any other functionalities of the QaaS app that should be improved?
  - Is there anything you would like to add?