Task 4 Notes

Suspicious Log requests (ID’s):

* 5zo6DEqnYN4zHDZYtbCXMt
* 5CJfYcJAMKAkhEQZLPAuTy
* mdB7yD2dp1BFZPontHBQ1Z (most suspicious)

Q1)

Is there a way for a hacker to access Daikibo's manufacturing status dashboard directly from the Internet?

You got it! In the original scope of the project we have listed that the dashboard will be living in Daikibo's Intranet. The only remote access to it would be through VPN tunnelling.

Q2)

Looking at the web\_requests.log - what is the user id with the most suspicious activity?

Nailed it! It starts off with a regular login -> browsing of the dashboard. But then it turns into a regular, once-per-hour (see the time stamps) automated check of the statuses in all 4 factories with no page resources being loaded and with an obviously non-human punctuality.