Task 3: SIEM

At the time of writing, it seems like the Splunk related labs are locked under a premium subscription. So I only managed to do the Introduction to SIEM lab instead. The provider that TryHackMe had us use was QRadar instead of Splunk.

The Incident: A case of cryptomining

Process that caused the alert: cudominer.exe

User that caused the alert: chris.fort

Hostname of suspect user: HR_02

Term that triggered the alert: miner