Updated Feb 12, 2023

Project 1 -OSQuery

🚀Surojit, your security engineering technical lead, has asked you to investigate a potential security tool called OSQuery. They have asked that you be prepared to demonstrate the application itself and its integration into the corporate EDR platform (wazuh). You are expected to demo your results to the full security engineering team in two weeks.

Your team's task (pick another student from the section or go it alone).

- Conduct some high level research on OSQuery so that you can explain what it does to your team at a high level
- Figure out how to Install OSQuery on either web01 (rocky) or wks01 (windows 10)
- Investigate and demonstrate some of the features of the OSQuery client application
- Figure out how to integrate OSQuery with Wazuh
- Develop an end to end demonstration that shows the triggering of an event that is picked up by OSQuery and how that event eventually makes it to Wazuh.
- Lastly, conclude by discussing any pros and cons of this tool and integration.

Deliverable 1. A demonstration video that touches base on all your team tasks. Provide a link to a highly professional video that the professor has access to. Under no circumstances, upload a video directly to CANVAS unless using CANVAS studio. If operating in a team, make sure both team members have a voice.

Deliverable 2. Provide a link to an exceptionally well prepared build document (this can be a google doc shared between team members or a github wiki entry) that covers the specific installation and configuration tasks associated with this project.

💡A word on teamwork and collaboration. Yes, all the teams in SEC350 are going after the same integration. Approach this project as though your team was in isolation, unaware that literally 35 other students were doing the same thing. If you or your team gets in trouble after working hard to figure out the issue, you may reach out to another team or student for assistance. If this is the case, please give them credit in your video and your build document.