Query Performance – Tuning & Monitoring

Pre-deployment	Deployment	Post-Deployment
osqueryi– Use osqueryi to prototype the query. If the query is taking a significant time to complete, dig deeper into what is causing the issue and continue iterating.	**Labels/Grouping** – Deploy new queries to groups of non-critical systems and monitor closely.	**Watchdog** – See watchdog limits below. If a query violates these constraints, it will be blocklisted for 24h, then tried again.
Profiler script – Use this python script to get an idea of what kind of performance hit the query will have on an endpoint. Make sure to run it on a system that has the same general specs as others in the target environment.	**Sharding** – Use sharding to deploy new queries to only a percentage of a group – useful for rolling out to a large amount of systems.	**Osquery_schedule** – This table will give you an overview of the currently scheduled queries, their performance metrics as well as whether or not the query has been blocklisted.

NetworkDefense.io

Feedback? Josh@DefensiveDepth.com
LearnOsquery.com

Osqueryd Watchdog Limits	Normal (0)	Restrictive (1)
CPU	**25% for 9 seconds**	**18% for 9 seconds**
Memory	**200MB**	**100MB**