There is some documentation on Suricata rules ([https://suricata.readthedocs.io/en/latest/rules/intro.html](https://suricata.readthedocs.io/en/latest/rules/intro.html)), and there have been trainings and a webinar ([https://www.youtube.com/watch?v=tvoqFBVSShA](https://www.youtube.com/watch?v=tvoqFBVSShA)), but we still miss a more complete guide which one can follow if they want to learn how to go from some malicious traffic to a rule that could detect such activity.

**Related issues:**
- Related to Documentation #1892: rule docs should include example rules
  
- Related to Documentation #4662: Add documentation section covering Suricata r...