Scenario

You’re a security analyst who must monitor traffic on your employer's network. You’ll be required to configure Suricata and use it to trigger alerts.

Here’s how you'll do this task: First, you'll explore custom rules in Suricata. Second, you'll run Suricata with a custom rule in order to trigger it, and examine the output logs in the **fast.log** file. Finally, you’ll examine the additional output that Suricata generates in the standard **eve.json** log file.

The tests you’ll run: you’ve been supplied with a **sample.pcap** file and a **custom.rules** file. These reside in your home folder.

Let’s define the files you’ll be working with in this lab activity:

- The **sample.pcap** file is a packet capture file that contains an example of network traffic data, which you’ll use to test the Suricata rules. This will allow you to simulate and repeat the exercise of monitoring network traffic.
- The custom.rules file contains a custom rule when the lab activity starts. You’ll add rules to this file and run them against the network traffic data in the sample.pcap file.
- The **fast.log** file will contain the alerts that Suricata generates. The fast.log file is empty when the lab starts. Each time you test a rule, or set of rules, against the sample network traffic data, Suricata adds a new alert line to the fast.log file when all the conditions in any of the rules are met. The fast.log file can be located in the /var/log/suricata directory after Suricata runs.The fast.log file is considered to be a depreciated format and is not recommended for incident response or threat hunting tasks but can be used to perform quick checks or tasks related to quality assurance.
- The **eve.json** file is the main, standard, and default log for events generated by Suricata. It contains detailed information about alerts triggered, as well as other network telemetry events, in JSON format. The eve.json file is generated when Suricate runs, and can also be located in the /var/log/suricata directory.

When you create a new rule, you'll need to test the rule to confirm whether or not it worked as expected. You can use the fast.log file to quickly compare the number of alerts generated each time you run Suricata to test a signature against the **sample.pcap** file.