# Examination of alerts, logs, and rules with Suricata

# Scenario:

# In this 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.

# Suricate provides pre-defined signature rules for alert logs and Network telemetry logs. Before we start from scratch it is better to use the custom rules to save time.

# Step1: Traverse from home folder to where Suricata exists using Cd Command

# Step 2: We examine the custom rule in Suricata using cat custom.rules

# It provides us with action ( alert/pass/reject) , Header (Signature’s network traffic) and rule options

# Step 3: Before we trigger we make sure that custom.rules doesn’t have the rules defined by using ls -l /var/log/suricata

# Step 4: sudo suricata -r sample.pcap -S custom.rules -k none provides how many packets were processed by suricata.

* The -r sample.pcap option specifies an input file to mimic network traffic. In this case, the sample.pcap file.
* The -S custom.rules option instructs Suricata to use the rules defined in the custom.rules file.
* The -k none option instructs Suricata to disable all checksum checks.

# Step 5: cat /var/log/suricata/filename.json returns the raw content of the file.

# Step 6 : To view the data in improved format and page by page we use jq . /var/log/suricata/eve.json | less

# Press Q to return to exit the screen from less command

# Sample:

# A screenshot of a computer screen Description automatically generated

# If we are willing to extract a specific event data we can use ,

# jq -c "[.timestamp,.flow\_id,.alert.signature,.proto,.dest\_ip]" /var/log/suricata/eve.json .

# A computer screen with white text and green numbers Description automatically generated

# We can also filter further based on flow\_id / timestamp etc..,