

Reviewing Suricata Alert Logs

First, I install Suricata using the APT package mgr:

```
analyst@936a371d7dde:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  libtcmalloc-minimal4
Recommended packages:
  snort-rules-default
The following NEW packages will be installed:
  suricata
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1964 kB of archives.
After this operation, 6634 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian-security bullseye-security/main amd64 suricata amd64 1:6.0.1-3+deb11u1 [1964 kB]
Fetched 1964 kB in 0s (14.7 MB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package suricata.
(Reading database ... 23441 files and directories currently installed.)
Preparing to unpack .../suricata_1%3a6.0.1-3+deb11u1_amd64.deb ...
Unpacking suricata (1:6.0.1-3+deb11u1) ...
Setting up suricata (1:6.0.1-3+deb11u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of restart.
Processing triggers for man-db (2.9.4-2) ...
analyst@936a371d7dde:~$
```

Next, I'll explore the custom rules file from the directory:

```
analyst@936a371d7dde:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;)
analyst@936a371d7dde:~$
```

This shows me the action type (alert), the protocol (http), src (\$Home_Net) & destination (\$External_Net) IP, the direction of the traffic (->), as well as the rule options etc:

```
analyst@936a371d7dde:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;)
analyst@936a371d7dde:~$
```

Based on the "content: GET" rule, this tells me whenever Suricata observes the text "GET" as the HTTP method, an alert will be triggered.

Capability	IDS	IPS	EDR
Detects malicious activity	✓	✓	✓
Prevents intrusions	N/A	✓	✓
Logs activity	✓	✓	✓
Generates alerts	✓	✓	✓
Performs behavioral analysis	N/A	N/A	✓

4 types of detection categories:

1. **A true positive** is an alert that correctly detects the presence of an attack.
2. **A true negative** is a state where there is no detection of malicious activity. This is when no malicious activity exists and no alert is triggered.
3. **A false positive** is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious, but it isn't. False positives are an inconvenience for security teams because they spend time and resources investigating an illegitimate alert.
4. **A false negative** is a state where the presence of a threat is not detected. This is when malicious activity happens but an IDS fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to.