Suricata Cheat Sheet | JQ commands for parsing Suricata NSM data

CHEAT SHEET

Use this cheat sheet for tips and tricks to select, filter and get rapid results from Suricata using JQ - the JSON command-line processing tool - by parsing standard Suricata eve.json logs. The commands covered in this cheat sheet are focused on the NSM data and protocol logs such as SMB, Anomaly, HTTP, DNS, TLS, Flow and others.

Select and show HTTP flows

```
jq -c 'select(.flow and .app_proto == "http")' eve.json
```

Display alerts only

```
jq -c 'select(.alert)' eve.json
```

Select DNS log records with TTL values between 0 and 100

```
jq 'select(.event_type=="dns")|select(.dns.ttl>0)|select(.dns.ttl<100)' | eve.json
```

List all DCERPC requests

```
jq 'select(.event_type=="dcerpc")|.dcerpc.request' eve.json
```

Select all protocol, flow, and alert records for flow_id: 1038930578016525

```
jq 'select(.flow_id==1038930578016525)' eve.json
```

Show all NTP flows

```
jq 'select(.event_type=="flow" and .app_proto=="ntp")' eve.json
```

Show TLS records with version TLSv1

```
jq 'select(.event_type=="tls" and .tls.version=="TLSv1")' eve.json
```

Display self signed certificates

```
jq 'select(.event_type=="tls" and .tls.subject==.tls.issuerdn)’ eve.json
```

Show DNS NXDOMAIN records

```
jq 'select(.event_type=="dns" and .dns.rcode=="NXDOMAIN")' eve.json
```

Show any SMB Anomaly event

```
jq 'select(.event_type=="anomaly" and .anomaly.app_proto=="smb")' eve.json
```

Sort and order per protocol and destination IP/Port

```
jq -c 'select(.flow)|[.dest_ip,.dest_port,.app_proto]' eve.json |sort|uniq -c|sort -nr|head
```

Show all destination IPs that have established flows with more than 10MB traffic to a client

```
jq 'select(.event_type=="flow" and .flow.state=="established" and .flow.bytes_toclient>10000000)|.dest_ip' eve.json
```

STAMVS NETWORKS
www.stamus-networks.com