Usecase 7: Facebook Access Detection

Objective: Create an alert when someone accesses Facebook

Log Source: Suricata

Event ID: N/A (Suricata custom rule)

Example Target Log From Suricata:


```
{"timestamp":"2025-03-
11T00:08:49.492974+0100","flow_id":1940109604699191,"in_iface":"\\Device\\NPF_
{56C83C56-73D7-441A-80D8-39DD27128F65}","event_type":"alert","src_ip":<source
ip>,"src_port":55582,"dest_ip":"<destination
ip>","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","tx_id":6,"alert":{"ac
tion":"allowed","gid":1,"signature_id":10000000,"rev":1,"signature":"DNS
Facebook","category":"Potential Corporate Privacy
Violation","severity":1},"dns":{"version":2,"query":[{"type":"query","id":4076
0,"rrname":"www.facebook.com","rrtype":"AAAA","tx_id":6,"opcode":0}]},"app_pro
to":"dns","direction":"to_server","flow":{"pkts_toserver":4,"pkts_toclient":3,
"bytes_toserver":381,"bytes_toclient":357,"start":"2025-03-
11T00:07:26.844932+0100","src_ip":"<source ip>","dest_ip":"<destination
ip>","src_port":55582,"dest_port":53}}
```


Pre-configuration: Suricata Windows Configuration: Involves installing with the wcap/ncap option> install ncap> go into the suricata.yaml file and change the home address to your address and change the interface to the windows interface name (both can be found through running ipconfig /all)> Add suricata to path variables (edit environment variables, environment variables, new, add path to suricata location)> can then run this command in powershell to run suricata suricata.exe -c <path to suricata.yaml file> -i <home ip address>

Custom Suricata Rule:

alert dns any any -> any any (msg:"DNS Facebook"; content:"facebook"; classtype:policy-violation; sid:10000000; rev: 1;)

creates an alert with the message “DNS facebook” when a DNS query containing the string “facebook” from any port/ip to any port/ip

Example Alerts:

	↓ timestamp	agent.name	rule.description	data.dns.answer.rrname	data.event_type
	Jul 5, 2025 @ 14:25:49.344	W11-Personal-Laptop	Suricata: Alert - DNS Facebook	www.facebook.com	alert
	Jul 5, 2025 @ 14:25:49.343	W11-Personal-Laptop	Suricata: Alert - DNS Facebook		alert
	Jul 5, 2025 @ 14:25:49.343	W11-Personal-Laptop	Suricata: Alert - DNS Facebook		alert
	Jul 5, 2025 @ 14:25:49.343	W11-Personal-Laptop	Suricata: Alert - DNS Facebook	star-mini.c10r.facebook.com	alert
	Jul 5, 2025 @ 14:25:49.227	W11-Personal-Laptop	Suricata: Alert - DNS Facebook	facebook.com	alert
	Jul 5, 2025 @ 14:25:49.223	W11-Personal-Laptop	Suricata: Alert - DNS Facebook	facebook.com	alert