**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":{"action":"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":40760,"rrname":"www.facebook.com","rrtype":"AAAA","tx\_id":6,"opcode":0}]},"app\_proto":"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:

A screenshot of a computer

AI-generated content may be incorrect.