SOC Use Case Report

UC-021: Rogue DNS Detection

Author	Abishek V
Date	3 Feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	DNS Logs / Network Telemetry
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-021
Use Case Name	Rogue DNS Detection
Category	Command and Control / Network Anomaly
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

Rogue DNS activity occurs when endpoints use unauthorized DNS servers or resolve domains outside approved resolvers. This behavior may indicate malware, tunneling, or policy bypass.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Expected DNS resolver: `192.168.56.1`
- Observed DNS server: `8.8.8.8`

SOC risk point: Malware often bypasses corporate DNS to evade filtering and detection.

3. Telemetry and Evidence

Primary logs

- DNS query logs
- Network flow logs
- Endpoint network telemetry

Key Indicators

Unauthorized Resolver	DNS queries to non-approved servers
Rare Domains	Newly registered or low-reputation domains
High Frequency	Repeated queries at regular intervals

4. Detection Logic

Trigger when:

- endpoint queries DNS servers not in approved list
- DNS traffic bypasses local resolver

Typical baselines:

- DNS queries should originate only to internal resolvers
- External DNS usage should be rare or blocked

5. SOC L1 Playbook

Phase A: Triage

1. Identify source host and DNS server IP

2. Validate whether DNS server is approved
3. Review volume and timing of DNS queries

Phase B: Investigation

1. Review domains queried via rogue DNS
2. Check domain reputation and age
3. Correlate with process and network activity
4. Identify possible DNS tunneling behavior
5. Scope for other endpoints using same DNS server

6. Evidence Timeline

Time	Source IP	DNS Server	Observation
05:36:12	192.168.56.110	8.8.8.8	DNS query observed
05:36:18	192.168.56.110	8.8.8.8	Repeated query pattern
05:36:30	192.168.56.110	Multiple	Queries to rare domains

Outcome: Endpoint using unauthorized DNS resolver. Activity requires validation and monitoring.

7. False Positive Checks

- user manually configured DNS for troubleshooting
- VPN client enforcing DNS changes
- temporary network configuration issues

8. Verdict Criteria

True Positive if:

- unauthorized DNS usage persists
- domains queried are suspicious or malicious
- activity correlates with other alerts

Persistent rogue DNS usage should be escalated for potential C2 investigation.

9. SOC Response Actions

- reset DNS configuration to baseline
- block unauthorized DNS servers at network layer
- scan endpoint for malware
- monitor DNS activity post-remediation

10. Ticket Notes

Ticket: UC-021 Rogue DNS Detected
Severity: Medium
Verdict: Under Investigation

Analyst Notes

- Detected DNS queries to unauthorized resolver.
- Observed repeated queries to rare domains.
- Endpoint placed under enhanced monitoring.