SOC Use Case Report

UC-022: Basic TOR Traffic Detection

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

1. Use Case Summary

Use Case ID	UC-022
Use Case Name	Basic TOR Traffic Detection
Category	Command and Control / Anonymization
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

TOR usage can indicate privacy-seeking behavior, but within enterprise environments it often represents policy violations or attempts to anonymize malicious activity.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Network behavior: Connections to known TOR entry nodes
- Protocols observed: TCP 9001 / 443

SOC risk point: TOR is frequently used to hide C2 communication and exfiltration paths.

3. Telemetry and Evidence

Primary logs

- Firewall logs
- Proxy logs
- Network flow telemetry

Key Indicators

Known TOR IPs	Matches threat intelligence lists
Unusual Ports	9001, 9050, 9150
Persistent Sessions	Long-lived encrypted connections

4. Detection Logic

Trigger when:

- outbound connections match known TOR node IPs
- encrypted traffic patterns align with TOR usage

Baselines:

- no TOR traffic expected from user endpoints
- TOR usage restricted to approved research systems (if any)

5. SOC L1 Playbook

Phase A: Triage

1. Identify source host and destination IP
2. Validate destination against TOR intelligence list
3. Determine duration and frequency of connections

Phase B: Investigation

1. Identify process initiating TOR traffic
2. Validate user intent and authorization
3. Check for concurrent suspicious activity
4. Scope for TOR usage on other endpoints

6. Evidence Timeline

Time	Source IP	Destination IP	Observation
06:14:05	192.168.56.110	TOR Node IP	Encrypted outbound connection
06:14:40	192.168.56.110	TOR Node IP	Persistent session maintained
06:15:10	192.168.56.110	Multiple	Additional TOR nodes contacted

Outcome: TOR traffic detected from endpoint. Activity requires authorization validation.

7. False Positive Checks

- approved research or security testing
- privacy tools used with explicit permission
- VPN misclassification (validate tunnel endpoints)

8. Verdict Criteria

True Positive if:

- TOR usage is unauthorized
- activity persists beyond brief testing
- correlated with suspicious behavior

Unauthorized TOR usage should be escalated if linked to data exfiltration or C2 activity.

9. SOC Response Actions

- block TOR nodes at network perimeter
- identify and remove TOR client software
- scan endpoint for malware
- document policy violation if applicable

10. Ticket Notes

Ticket: UC-022 TOR Traffic Detected
Severity: Medium
Verdict: Under Investigation

Analyst Notes

- Observed outbound connections to known TOR entry nodes.
- Traffic pattern consistent with TOR usage.
- Endpoint placed under investigation pending authorization confirmation.