

SOC Use Case Report

UC-025: Identifying Web Users by Country

Author	Abishek V
Date	5 Feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Proxy / Firewall / Geo-IP Enrichment
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-025
Use Case Name	Identifying Web Users by Country
Category	Network Monitoring / Geo-Anomaly
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Low → Medium

Geo-location analysis helps SOC teams identify anomalous access patterns, policy violations, and potential account compromise involving foreign regions.

2. Scenario

- Endpoint: Windows 10 (192.168.56.110)
- User: `clair`
- Traffic type: Web browsing
- Observed locations: India (baseline), Eastern Europe (anomaly)

SOC risk point: Sudden web activity from unexpected geographies may indicate VPN abuse, credential misuse, or proxy evasion.

3. Telemetry and Evidence

Primary logs

- Proxy logs
- Firewall logs
- Geo-IP enriched network telemetry

Key Indicators

Unexpected Country	Traffic outside user baseline geography
Impossible Travel	Rapid country switching
High-Risk Regions	Traffic from sanctioned or high-risk zones

4. Detection Logic

Trigger when:

- web traffic originates from uncommon or restricted countries
- geographic pattern deviates from user baseline

5. SOC L1 Playbook

Phase A: Triage

1. Identify user and source IP
2. Review geo-location of traffic
3. Compare against known baseline

Phase B: Investigation

1. Validate use of VPN or proxy
2. Check authentication and session history
3. Correlate with login and endpoint activity
4. Scope for similar behavior across users

6. Evidence Timeline

Time	Source IP	Country	Observation
09:41:22	192.168.56.110	India	Normal web activity
09:46:58	203.0.113.45	Romania	Unexpected web session

Outcome: Web activity observed from unexpected geography. Validation required.

7. False Positive Checks

- corporate VPN usage
- remote travel or roaming user
- CDN or proxy misattribution

8. Verdict Criteria

True Positive if:

- geo-anomaly persists without explanation
- activity correlates with other alerts

9. SOC Response Actions

- validate user location and intent
- enforce geo-based access restrictions
- reset credentials if compromise suspected

10. Ticket Notes

Ticket: UC-025 Web Users by Country
Severity: Low
Verdict: Under Investigation