SOC Use Case Report

UC-023: Detecting Unencrypted Web Communications

Author	Abishek V
Date	4 Feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Proxy / Firewall / Network Logs
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-023
Use Case Name	Detecting Unencrypted Web Communications
Category	Network Security / Data Exposure
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium

Unencrypted web traffic exposes credentials and sensitive data. SOC L1 must identify whether HTTP usage is legitimate, misconfigured, or malicious.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Traffic type: HTTP (cleartext)
- Destination: External web server

SOC risk point: Attackers often use HTTP for command-and-control or data exfiltration to evade inspection.

3. Telemetry and Evidence

Primary logs

- Proxy logs
- Firewall logs
- Network flow telemetry

Key Indicators

Port 80 Traffic	Cleartext HTTP sessions
Credential Exposure	Login forms over HTTP
Unusual Destinations	Rare or newly registered domains

4. Detection Logic

Trigger when:

- outbound web traffic uses HTTP instead of HTTPS
- sensitive data transmitted over cleartext

5. SOC L1 Playbook

Phase A: Triage

1. Identify source endpoint and destination
2. Confirm protocol and port
3. Check frequency and volume

Phase B: Investigation

1. Identify application generating traffic
2. Validate destination reputation
3. Check for authentication or data transfer
4. Scope similar behavior across environment

6. Evidence Timeline

Time	Source IP	Destination	Observation
07:11:04	192.168.56.110	external-site.com	HTTP request observed
07:11:20	192.168.56.110	external-site.com	Cleartext POST request

Outcome: Unencrypted web communication detected. Monitoring and validation required.

7. False Positive Checks

- legacy internal applications
- test or development environments
- approved exception list

8. Verdict Criteria

True Positive if:

- sensitive data transmitted in cleartext
- destination is untrusted

9. SOC Response Actions

- block HTTP traffic where possible
- enforce HTTPS via policy
- notify application owners

10. Ticket Notes

Ticket: UC-023 Unencrypted Web Traffic
Severity: Medium
Verdict: Under Investigation