SOC Use Case Report

UC-024: Finding Large Web Uploads

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

1. Use Case Summary

Use Case ID	UC-024
Use Case Name	Finding Large Web Uploads
Category	Data Exfiltration / Network Anomaly
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

Large outbound uploads may indicate data exfiltration. SOC L1 must determine if uploads are legitimate business activity.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Upload size: >100 MB
- Destination: External cloud service

SOC risk point: Attackers often exfiltrate data over HTTPS to evade inspection.

3. Telemetry and Evidence

Primary logs

- Proxy logs
- Firewall logs
- Network flow telemetry

Key Indicators

High Upload Volume	Unusual outbound data size
Rare Destination	Cloud or unknown service
Off-Hours Activity	Uploads outside business hours

4. Detection Logic

Trigger when:

- upload size exceeds baseline
- repeated large uploads occur in short time window

5. SOC L1 Playbook

Phase A: Triage

1. Identify source endpoint and user
2. Confirm upload size and destination
3. Check time of activity

Phase B: Investigation

1. Identify application or browser used
2. Validate destination legitimacy
3. Correlate with file access activity
4. Scope similar uploads across environment

6. Evidence Timeline

Time	Source IP	Destination	Observation
08:52:14	192.168.56.110	cloud-storage.com	120MB upload detected
08:53:02	192.168.56.110	cloud-storage.com	Upload completed

Outcome: Large outbound upload detected. Validation with user required.

7. False Positive Checks

- legitimate cloud backup
- approved file sharing services
- business data transfer

8. Verdict Criteria

True Positive if:

- upload destination is unapproved
- data accessed prior is sensitive

9. SOC Response Actions

- block destination if malicious
- initiate data loss investigation
- notify data protection team

10. Ticket Notes

Ticket: UC-024 Large Web Upload Detected
Severity: Medium
Verdict: Under Investigation